
Untersuchung der Anwendbarkeit von Methoden zur Evaluierung der IT-Sicherheit auf KMU-Webshops

An analysis of the applicability of IT security evaluations for SME online shops

Bachelor-Thesis von Christian Fritz

19. Oktober 2010



Untersuchung der Anwendbarkeit von Methoden zur Evaluierung der IT-Sicherheit auf KMU-Webshops

Genehmigte Bachelor-Thesis von Christian Fritz

Gutachten: Dr. Melanie Volkamer

Tag der Einreichung:

Technische Universität Darmstadt
Fachbereich Informatik

Center for Advanced Security Research Darmstadt (CASED)
Dr. Melanie Volkamer

Erklärung zur Bachelor-Thesis

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 19. Oktober 2010

(C. Fritz)

Zusammenfassung

Moderne Informationstechnologie wird heutzutage in vielen Unternehmen zur Verarbeitung von geschäftsrelevanten Daten eingesetzt. Dies trifft vor allem auf Webshops zu, deren gesamtes Geschäftsmodell vom Internet abhängig ist. Dadurch entstehen neue Gefährdungen: Neben technischen Defekten stellen Angriffe über das Internet das größte Risiko dar. Die notwendige Absicherung der IT-Infrastruktur ist für viele Webshops eine Herausforderung, da sie zu den kleinen und mittleren Unternehmen (KMUs) gehören, das heißt sie verfügen über einen geringen bis mittleren Umsatz sowie wenige Mitarbeiter und können daher wenige Ressourcen für die IT-Sicherheit bereitstellen.

Ein erster Schritt zur Verbesserung der IT-Sicherheit ist eine Analyse der bestehenden Maßnahmen, auf deren Grundlage dann das weitere Vorgehen geplant werden kann. In der vorliegenden Arbeit werden verschiedene Ansätze untersucht, mit denen die IT-Sicherheit in einem KMU-Webshop evaluiert werden kann. Dabei werden sowohl die Charakteristika von KMUs wie ihre geringe Finanzkraft, die wenigen Mitarbeiter und ihre Flexibilität aufgrund flacher Hierarchien als auch der Aufbau und die Eigenschaften von Webshops berücksichtigt.

In der Arbeit wurden Standards als Möglichkeit zur Evaluierung und Verbesserung der IT-Sicherheit analysiert. Sie bieten etablierte Methoden, sind aber oft sehr umfangreich und decken neben der Infrastruktur auch organisatorische Aspekte ab. Bekannte Beispiele hierfür sind der IT-Grundschutz oder die ISO/IEC 27001 Norm, die beide ein Managementsystem für Informationssicherheit bereitstellen. Auch IT-Governance- und IT-Service-Standards, die nur nebensächlich auf die Sicherheit eingehen, werden bezüglich ihrer Anwendbarkeit zur Evaluierung der IT-Sicherheit von Webshops bewertet.

Des Weiteren werden Online-Gütesiegel betrachtet. Es gibt zwei verschiedene Arten, die untersucht werden: Einerseits Gütesiegel, die sich auf Webshops spezialisiert haben: Ihr Ziel ist hauptsächlich, einen verbraucherfreundlichen und vertrauenswürdigen Webshop zu kennzeichnen, dabei spielt auch der Sicherheitsaspekt eine Rolle. Andererseits gibt es Datenschutz-Gütesiegel, die allgemein auf technische Systeme ausgerichtet sind und auf die rechtlichen Aspekte des Datenschutzes fokussiert sind. Eine Auflistung und Analyse der bekanntesten und relevanten Gütesiegel zeigt, dass die von ihnen gestellten Anforderungen an die IT-Sicherheit ähnlich sind.

Schließlich werden Sicherheitsaudits, Checklisten und Fragebögen sowie Analyseprogramme hinsichtlich ihrer Anwendbarkeit zur Evaluation der IT-Sicherheit von Webshops evaluiert. Sie bieten in der Regel keine Zertifikate für das festgestellte Schutzniveau. Sicherheitsaudits können intern von eigenen Mitarbeitern oder extern von einem Dienstleister durchgeführt werden. Sie können - wie auch Checklisten und Fragebögen, die in der Regel intern bearbeitet werden - alle Ebenen des Unternehmens überprüfen, während Analyseprogramme nur die technische Ebene auf Schwachstellen untersuchen können.

Angesichts der Seitenbedingungen wie der geringen finanziellen Möglichkeiten und des fehlenden Expertenwissens ist es schwierig, eine klare Empfehlung für eine der Methoden zu geben. Viele der Standards sind für KMU-Webshops ungeeignet, andere zu aufwändig. Die empfehlenswerten Vertreter der Gütesiegel prüfen einige sicherheitskritische Faktoren, lassen aber wichtige Details auf technischer Ebene wie Schwachstellen gegen XSS-Angriffe unberücksichtigt. Die Qualität der Sicherheitsaudits, Fragebögen, Checklisten und Analyseprogramme ist sehr stark abhängig vom Anbieter. Diese Methoden sind auch für kleinere KMU-Webshops nicht zu aufwändig. Daher sind Fragebögen und Checklisten eine einfache Methode, um grundlegende Sicherheitsmaßnahmen zu überprüfen. Analyseprogramme sind zu empfehlen, um Sicherheitslücken auf Hardware- und Software-Ebene kostengünstig aufzuspüren. Für Webshops mit wenig Wissen über IT-Sicherheit ist ein extern durchgeführter Sicherheitsaudit die komfortabelste Lösung, um das Sicherheitsniveau zu analysieren.

Welche Evaluationsmethode die Richtige ist, hängt stark von der Infrastruktur des Webshops ab. Auch die zur Verfügung stehenden Ressourcen, besonders die Arbeitszeit, das investierte Geld und das Wissen der Mitarbeiter im Bereich IT-Sicherheit, sind wichtige Faktoren bei der Auswahl der Methode.

Inhaltsverzeichnis

1	Einleitung	7
1.1	Motivation	7
1.2	Ziel	7
1.3	Aufbau	8
1.4	Methodik	8
2	Kleine und mittlere Unternehmen	10
2.1	Definitionen	10
2.2	Auswirkungen auf die IT-Sicherheit	10
3	Webshops	12
3.1	Aufbau	12
3.1.1	Hardware	14
3.1.2	Software	14
3.1.3	Bezahl-Schnittstelle	15
3.1.4	Bezahlungssysteme	16
3.2	Sicherheitsbetrachtung	16
3.2.1	Rechtliche Anforderungen	17
3.2.2	Schutzziele	18
3.2.3	Gefährdungen	18
4	Standards	22
4.1	ISO/IEC 27001	22
4.2	ISO 27001 basierend auf IT-Grundschutz	25
4.3	Payment Card Industry Data Security Standard	29
4.4	OCTAVE	32
4.5	ITIL	33
4.6	Cobit	36
4.7	IDW PS 330	38
4.8	Common Criteria	40
5	Gütesiegel	42
5.1	Initiative D21	42
5.1.1	Trusted Shops	43
5.1.2	S@fer Shopping	44
5.1.3	Internet Privacy Standards	45
5.1.4	EHI Geprüfter Online-Shop	46
5.2	Weitere Webshop-Gütesiegel	48
5.3	Datenschutz-Gütesiegel	49
5.3.1	ULD-Datenschutz-Gütesiegel	49
5.3.2	Datenschutz-Gütesiegel der Freien Hansestadt Bremen	51
5.3.3	Europäisches Datenschutz-Gütesiegel	52
6	Sonstige Sicherheitsüberprüfungen	54
6.1	Fragebögen und Checklisten	54

6.2	Analyseprogramme	56
6.3	Sicherheits-Audits	58
7	Analyse	61
7.1	Eignung von Standards	63
7.2	Eignung von Gütesiegeln	64
7.3	Eignung von sonstigen Sicherheitsüberprüfungen	66
7.4	Ergebnis der Analyse	66
8	Fazit und Ausblick	68
	Literaturverzeichnis	70

Abbildungsverzeichnis

1.3.1 Übersicht und thematischer Zusammenhang der Kapitel	8
1.4.1 Struktur des Templates	9
3.1.1 Schematische Darstellung des Aufbaus eines Webshops ²	13
3.1.2 Schematische Darstellung der Shop-Software mit zusätzlichen Modulen	14
3.1.3 Beispiele für Online-Bezahlsysteme ⁸	16
3.2.1 Die Kontrollen aus der Anlage zu §9 Satz 1 des BDSG	17
3.2.2 Angriffsbaum zur Verfügbarkeit	19
3.2.3 Angriffsbaum zur Vertraulichkeit	19
3.2.4 Angriffsbaum zur Integrität	20
4.1.1 Die Bereiche der ISO 27002 Norm ²	23
4.1.2 Der PDCA-Zyklus von ISO 27001 (S. 38, [24])	24
4.2.1 Die Vorgehensweise nach Grundsatz-Methodik	26
4.3.1 Die 12 Anforderungen von PCI DSS	30
4.4.1 Einordnung von OCTAVE in einen generischen Risikomanagement-Prozess (aus [1])	32
4.5.1 ITIL Service Lifecycle (vereinfacht, aus [38])	34
4.6.1 Überblick über das Cobit-Framework, entnommen aus [20]	36
6.1.1 Die Phasen des ENISA-Fragebogens für Kleinstunternehmen	55
6.1.2 Die 10 Maßnahmen von InfoSurance für einen wirkungsvollen Grundsatz	56
7.0.1 Grobe Einordnung der Methoden anhand der technischen Fokussierung	61
7.0.2 Grobe Einordnung der Methoden anhand der organisatorischen Fokussierung	61
7.0.3 Einordnung der Methoden nach dem Kriterium „Kosten“	62
7.0.4 Einordnung der Methoden nach dem Kriterium „Aufwand“	62
7.0.5 Einordnung der Methoden nach dem Kriterium „benötigtes Wissen“	63

Tabellenverzeichnis

2.1	Definition von KMUs der EU von 2005 [28]	10
2.2	Definition von KMUs des IfM Bonn von 2002 ¹	10
3.1	Auflistung einiger gängiger Verkaufsportale und ihrer Sicherheitseigenschaften ⁵	15
4.1	Die ISO 27000-Normenfamilie	23
4.2	Tabelle zu BSI-Standards aus [19]	26
4.3	Schichten des IT-Grundschutzmodells aus [19]	27
4.4	Tabelle zur Auswahl des Selbstbeurteilungsfragebogens aus [30]	30
4.5	Auflagen des PCI-Standards für unterschiedliche Level	31
4.6	Evaluation Assurance Levels	40
4.7	Klassen der Sicherheitsanforderungen	41
5.1	Kosten für das EHI-Gütesiegel ¹¹	47
5.2	Die Bestandteile des allgemeinen Anforderungsprofils des Anforderungskatalogs [8]	50
7.1	Vergleich der Gütesiegel	65

1 Einleitung

1.1 Motivation

Viele Unternehmen nutzen moderne Informationstechnologie zur Speicherung und Verarbeitung von geschäftsrelevanten Daten. Besonders Webshops sind auf die IT angewiesen, da sie im Gegensatz zum traditionellen Einzelhandel ihren Umsatz ausschließlich über das Internet generieren. Für sie muss gewährleistet sein, dass sie ihre Produkte möglichst unterbrechungsfrei präsentieren und verkaufen können. Ein Datenverlust oder der Ausfall von Komponenten stellt somit eine Bedrohung für die Geschäftstätigkeit dar. Neben technischen Defekten ist aber vor allem die notwendige Anbindung an das Internet ein Risiko für die Infrastruktur der Webshops: Laut einer weltweiten Studie der Symantec Corporation [6] erlebten 75 % der befragten Unternehmen in einem Zeitraum von zwölf Monaten Angriffe über das Internet, 29 % sagten aus, dass die Anzahl im Vergleich zum letzten Jahr zugenommen hat.

Ziele der Angriffe sind unter anderem das Ausspähen von Kundendaten oder wichtigen Informationen und das Eindringen, Übernehmen oder Abschalten des Systems. Ein erfolgreicher Angriff bedeutet für einen Webshop deshalb einen Vertrauensverlust bei den Kunden sowie möglicherweise Ausfallzeiten, in denen der Webshop nicht erreichbar ist und daher keinen Umsatz erzielen kann. Daher muss der zum Betrieb benötigten Infrastruktur, die sich meist aus Hard- und Software-Komponenten zusammensetzt, besondere Aufmerksamkeit bei der Absicherung gegen Bedrohungen gewidmet werden.

Eine zusätzliche Herausforderung für kleine und mittlere Unternehmen (KMUs), zu denen auch die meisten Webshops gehören, ist das geringe Kapital, welches sie den Bedrohungen entgegensetzen können: Während größere Unternehmen genug Kapital besitzen, um eine eigene Abteilung zu beschäftigen, die sich intensiv um die Aktualisierung, Absicherung und Wartung der IT kümmert, müssen KMUs ihr Kapital projektbezogen investieren und Investitionen in IT-Sicherheit nebenher ansparen (S. 52, [26]). Daher müssen sie die wenigen Mittel, die ihnen für Sicherheitsmaßnahmen zur Verfügung stehen, effektiv einsetzen. Sie sind finanziell nicht in der Lage, umfangreiche Sicherheitsanweisungen durchzusetzen und haben nicht die nötigen Mitarbeiter, die sich in diesen Themen spezialisieren können. Gerade deshalb muss versucht werden, die vorhandenen Ressourcen wirksam zum Erreichen des gewünschten Sicherheitsniveaus einzusetzen.

Viele KMUs haben bereits einzelne Maßnahmen zur Absicherung der IT-Sicherheit ergriffen, aber es gibt auch Methoden, die bisher von wenigen KMUs eingesetzt werden¹. Ein erster Schritt zur Verbesserung der IT-Sicherheit ist deshalb zunächst die Bestimmung des bisherigen Schutzniveaus.

1.2 Ziel

Ein Webshop kann verschiedene Ansätze aufgreifen, um die IT-Sicherheit seiner Infrastruktur zu analysieren und zu verbessern. Neben der Anwendung von Standards der IT-Sicherheit, die oft alle Bereiche des Webshops auswerten und verbessern, bieten auch Gütesiegel eine Überprüfung und Zertifizierung. Eine günstigere, aber auch weniger vergleichbare Möglichkeit sind nicht zertifizierte Sicherheitsaudits. Diese können - je nach Komplexität - entweder mit Hilfe von externen Dienstleistern oder durch Mitarbeiter des Unternehmens durchgeführt werden. Ziel dieser Arbeit ist es, die verschiedenen Evaluationsansätze nach Kriterien wie Wirksamkeit und Aufwand hinsichtlich ihrer Anwendbarkeit für KMU-Webshops zu analysieren und optimale Verfahren zur Bewertung der Sicherheit der IT-Infrastruktur zu identifizieren. Neben den Bedrohungen, die sich durch die Anbindung an das Internet ergeben, müssen die Charakteristika der Organisation und der IT-Infrastruktur berücksichtigt werden. Diese werden sowohl durch die

¹ Beispielsweise physischer Schutz oder Notfallpläne, siehe [9].

Eigenschaften von KMUs als auch durch den Aufbau der Webshops definiert. Bei der Analyse werden auch mögliche Seiteneffekte der Verfahren, wie beispielsweise Verbesserungen des Sicherheitsniveaus und ein Vertrauensgewinn bei Kunden, berücksichtigt.

1.3 Aufbau

Nach der Einleitung (Kapitel 1) mit der Beschreibung von Motivation, Ziel und Aufbau werden in den nächsten zwei Kapiteln grundlegende Begriffe erläutert: Zunächst wird in Kapitel 2 definiert, was unter kleinen und mittleren Unternehmen zu verstehen ist und welche Eigenschaften sie besitzen, die für die Analyse der Methoden wichtig sind. Danach folgt in Kapitel 3 eine Definition des Begriffs „Webshop“ sowie der Aufbau und eine Sicherheitsbetrachtung von Webshops.

Die folgenden drei Kapitel beschreiben ausgewählte Standards (Kapitel 4), Gütesiegel (Kapitel 5) und sonstige Sicherheitsüberprüfungen (Kapitel 6) nach einem im Rahmen dieser Arbeit definierten Templates, welches in Sektion 1.4 erläutert wird. Anschließend wird ausgehend von den Eigenschaften der Webshop-KMUs und den gesammelten Informationen über die Methoden eine Analyse durchgeführt, die die Anwendbarkeit der Methoden bewertet (Kapitel 7). Schließlich werden die Erkenntnisse zusammengefasst und ein Ausblick gegeben. Der Zusammenhang zwischen den Kapiteln ist in Abbildung 1.3.1 visualisiert.

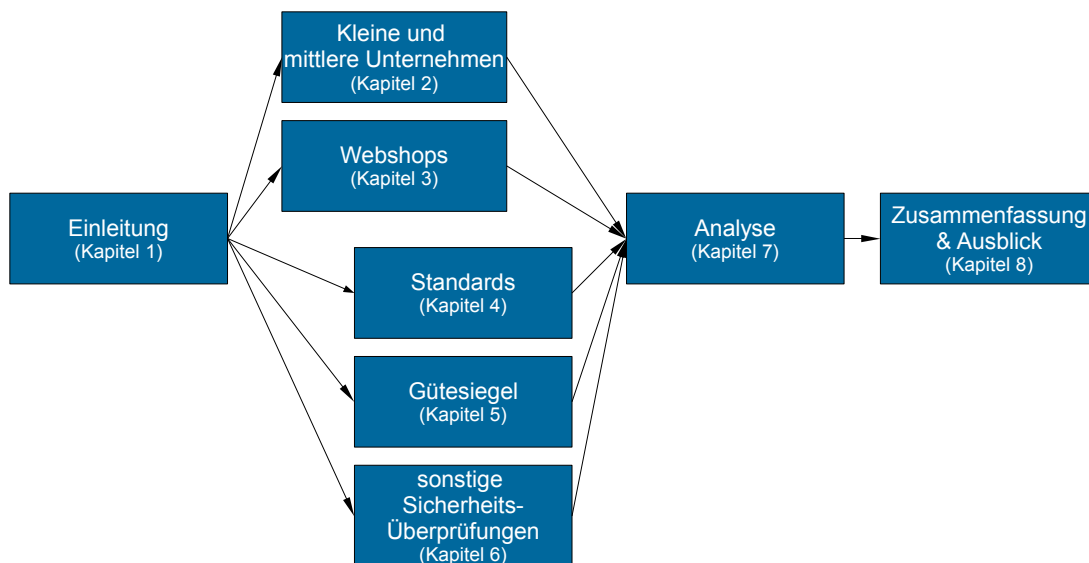


Abbildung 1.3.1: Übersicht und thematischer Zusammenhang der Kapitel

1.4 Methodik

Zur besseren Vergleichbarkeit der unterschiedlichen vorgestellten Methoden wurde ein Template zur Beschreibung von Standards, Gütesiegeln und sonstigen Sicherheitsüberprüfungen erstellt. Es enthält die in Abbildung 1.4.1 aufgelisteten Kriterien, die im Folgenden genauer erklärt werden.

Zunächst werden *allgemeine Daten* der Methode dargestellt. Falls vorhanden, beinhaltet dies Informationen über ihren Ursprung, ihre Verbreitung und die Anzahl der bisherigen Zertifizierungen. Außerdem wird ein Überblick über den Aufbau der Methode gegeben. Dabei handelt es sich unter anderem um die Anforderungen des Prüfverfahrens oder die Beschreibung von einzelnen Phasen, die zur Durchführung der Methode notwendig sind.

Danach wird die *Ebene* beschrieben, das heißt ob die Methode eher auf technischer oder organisatorischer Ebene ansetzt. Es wird beispielsweise unterschieden zwischen eher technischen Maßnahmen für spezifische Komponenten und einem übergreifenden Management-Konzept.

Der Abschnitt *Voraussetzungen* befasst sich mit den Bedingungen, die die Methode an das Unternehmen stellt, dies kann unter anderem eine bestimmte Organisationsform sein - zum Beispiel können einige der Gütesiegel nur auf Webshops angewendet werden. Eine andere mögliche Vorbedingung ergibt sich durch Methoden, die auf bestimmte Infrastruktur oder Daten ausgelegt sind. Ohne diese ist der Standard meist nur teilweise umsetzbar.

Als nächstes folgt eine Beschreibung der *Prüfung*, dazu gehören Details zum Prüfungsverfahren, den Prüfern und Prüfungsbescheinigungen. Falls ein Zertifikat ausgestellt wird, werden die Gültigkeitsdauer und weitere Besonderheiten wie regelmäßige Überprüfungen oder vereinfachte Rezertifizierungen aufgelistet.

Im Abschnitt *Aufwand und Kosten* werden die beiden für KMUs wichtigen Auswahlkriterien dokumentiert, hierbei wird zwischen einmaligen und regelmäßigen Kosten differenziert und die Dauer des Prüfungsprozesses sowie der Aufwand für die Mitarbeiter berücksichtigt.

Zuletzt wird der *Nutzen* für die Evaluation und Verbesserung der IT-Sicherheit von KMU-Webshops und die *Anpassbarkeit* an diese Art von Unternehmen beschrieben. Ein wichtiges Kriterium dafür ist die Existenz von Änderungsmöglichkeiten, Vereinfachungen oder optionalen Arbeitsschritten im Verfahren, die das vorausgesetzte Wissen oder die benötigten Ressourcen verringern.

In der Analyse werden die Methoden zunächst nach technischem und organisatorischem Schwerpunkt geordnet. Anschließend werden sowohl Methoden gleichen Typs untereinander (zum Beispiel verschiedene Gütesiegel) als auch unterschiedliche Methoden verglichen und bewertet.

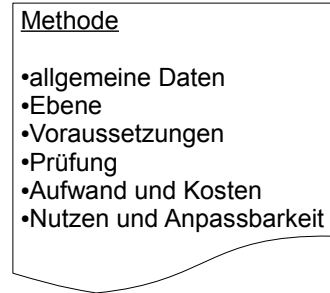


Abbildung 1.4.1: Struktur des Templates

2 Kleine und mittlere Unternehmen

2.1 Definitionen

Es gibt mehrere Definitionen von kleinen und mittleren Unternehmen (KMUs), denen unterschiedliche Motivationen zugrunde liegen. Sie haben verschiedene Formen, meistens werden sie aber über die Mitarbeiteranzahl und den Umsatz definiert. Während in mehreren Ländern für Dienstleistungs- und Produktionsgewerbe unterschiedliche Grenzen gesetzt werden, ist das in den beiden folgenden Definitionen, die in Deutschland am meisten verbreitet sind, nicht der Fall.

Tabelle 2.1 zeigt eine Definition der Europäischen Union von 2005 [28]. Ein Unternehmen ist ein KMU nach EU-Definition, wenn die Mitarbeiterzahl und entweder der Jahresumsatz oder die Bilanzsumme die in der Tabelle angegebenen Werte nicht überschreiten. Im Gegensatz zur Definition des Instituts für Mittelstandsforschung Bonn (IfM)¹, die in Tabelle 2.2 aufgeführt ist, trifft die Kategorisierung durch strengere Kriterien auf weniger Unternehmen zu. Nach der IfM-Definition sind 99,7 % der Unternehmen in Deutschland KMUs, sie machten 2007 aber nur 37,5 % des Umsatzes aus².

Art des Unternehmens	Mitarbeiterzahl	Jahresumsatz in Euro	Bilanzsumme in Euro
Kleinstunternehmen	< 10	<= 2 Mio.	<= 2 Mio.
kleines Unternehmen	< 50	<= 10 Mio.	<= 10 Mio.
mittleres Unternehmen	< 250	<= 50 Mio.	<= 43 Mio.

Tabelle 2.1: Definition von KMUs der EU von 2005 [28]

Art des Unternehmens	Mitarbeiterzahl	Jahresumsatz in Euro
kleines Unternehmen	< 10	< 1 Mio.
mittleres Unternehmen	< 500	< 50 Mio.

Tabelle 2.2: Definition von KMUs des IfM Bonn von 2002¹

2.2 Auswirkungen auf die IT-Sicherheit

KMUs haben spezielle Charakteristika, die sich auf ihre IT-Sicherheit auswirken. Einige wirken positiv, aber die Mehrzahl führt zu Problemen oder Herausforderungen.

Aufgrund der geringen Mitarbeiterzahl haben KMUs flache Hierarchien, was ein wichtiger Faktor für die Flexibilität solcher Firmen ist, da neue Richtlinien so schnell umsetzbar sind (S. 44, [26]). Allerdings haben die Mitarbeiter von KMUs in der Regel ein breiteres Aufgabenfeld als Mitarbeiter in größeren Firmen. Dies kann sich beispielsweise darin äußern, dass der Datenschutzbeauftragte oder ein Mitarbeiter, der für die IT-Sicherheit verantwortlich ist, noch andere Aufgaben zu erledigen hat und daher weniger spezialisiert ist als die Fachkräfte von größeren Unternehmen. Bedingt durch den geringeren Umsatz haben KMUs weniger Kapital als größere Unternehmen zur Verfügung. Dies kann bei der Umsetzung von größeren IT-Sicherheitsmaßnahmen zu Problemen führen, da weder das Know-How der Mitarbeiter

¹ <http://www.ifm-bonn.org/index.php?id=89>, aufgerufen am 22.08.2010.

² <http://www.ifm-bonn.org/index.php?id=99>, aufgerufen am 22.08.2010.

noch ausreichend Geld vorhanden ist, um die komplette Umsetzung durch externe Dienstleister erledigen zu lassen.

Die benutzte Infrastruktur ist bei KMUs länger in Betrieb als in größeren Unternehmen. Dies stellt ein Sicherheitsrisiko dar, da veraltete Technik fehleranfälliger ist oder allgemein bekannte Angriffe gegen sie vorhanden sind. Laut einer Studie der Zürcher Hochschule [23] sind die Lebenszyklen von Software bei über 60 % der KMUs länger als 3 Jahre, ca. 90 % der KMUs haben Hardware-Lebenszyklen mit einer Länge von mehr als 3 Jahren.

Einfache Basis-Schutzmaßnahmen werden von vielen KMUs schon umgesetzt: Eine Befragung von 600 Kleinunternehmen (weniger als 50 Mitarbeiter) in Deutschland hat 2007 ergeben, dass 93 % eine Antivirenlösung und ebenfalls 93 % eine Firewall einsetzen, 81 % der Unternehmen haben einen Spam-Filter [39]. Dies wird durch ähnliche Ergebnisse (81 % der befragten Unternehmen setzen Firewalls ein, 94 % benutzen Antivirenprogramme) in einer weiteren KMU-Studie zu IT-Sicherheit [9] bestätigt, hier wurden 40 Unternehmen aus Europa befragt, die weniger als 250 Mitarbeiter beschäftigen. Die Studie deckt aber auch auf, dass nur 29% der Unternehmen Maßnahmen für den physischen Schutz ergriffen haben, also zum Beispiel Zutrittskontrolle und gesicherte Serverräume. Ein weiteres Ergebnis der Studie, bei dem nicht nur Antworten der 40 Unternehmen aus Europa, sondern auch weiteren 81 Unternehmen aus der USA einfließen, zeigt, dass bei nur 25 % der Unternehmen die Sicherheitsverantwortlichen anerkannte IT-Sicherheitsqualifikationen besitzen.

Aufgrund der Kosten lagern mehr und mehr Unternehmen ihre IT-Abteilung an externe Dienstleister aus³. Dieses Outsourcing kann zu Kostenvorteilen und Qualitätssteigerung führen. Vor allem Unternehmen, die aus einem Geschäftsbereich stammen, der wenig mit IT zu tun hat, können sich so auf ihre Kernkompetenzen konzentrieren. Aber selbst bei Auslagerung der Infrastruktur darf nicht vernachlässigt werden, dass neben der Technik auch der Mensch ein Sicherheitsrisiko ist. So können Mitarbeiter durch fahrlässiges Verhalten Angriffe oder Diebstahl von Daten ermöglichen. Dass dies ein ernst zu nehmendes Risiko ist, zeigt auch eine Studie, in der 58,4 % der befragten Unternehmen angegeben haben, dass „leichtfertiger Umgang von Mitarbeitern mit Sicherheitsstandards“ eine der größten Bedrohungen für die IT darstellt (S. 36, [14]).

³ http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_2010_-_13_01_2010.pdf, aufgerufen am 19.09.2010.

3 Webshops

Als Webshop wird in dieser Arbeit ein Internetangebot, üblicherweise in Form einer Webseite, bezeichnet, das es Kunden ermöglicht, durch eine Transaktion Produkte zu erwerben. Dabei ist unerheblich, ob diese Produkte in digitaler Form vorliegen (zum Beispiel als Software-Download) oder physikalisch an den Empfänger übermittelt werden müssen.

Dies bedeutet, dass der Kunde auf der Webseite die Möglichkeit haben muss, einen Kaufvertrag abzuschließen. Dafür muss der Kunde ein Angebot auswählen und den Kauf bestätigen, sodass eine rechtsgültige Vereinbarung getroffen wird. Dies wird meistens durch einen virtuellen Warenkorb, eine virtuelle Kasse und vorgegebene Zahlungsmodalitäten umgesetzt. Die hier betrachteten Webshops basieren in erster Linie auf einer B2C-Handelsbeziehung („Business to Consumer“), bei der ein Unternehmen Verbrauchern Produkte anbietet (S. 85, [3]).

Kleine bis mittelgroße Webshops fallen oft unter die im vorigen Kapitel erläuterte KMU-Definition. Diese Einordnung wird vor allem durch ihre Organisationsstruktur begünstigt: Die Unterhaltung eines Webshops benötigt im Vergleich zu traditionellen Shops weniger Mitarbeiter, Prozesse wie der Bezahlvorgang werden elektronisch durchgeführt, die Warenübergabe wird in der Regel von Paketdiensten übernommen. Des Weiteren ist es gerade für kleinere Webshops sehr einfach möglich, kritische Geschäftsbereiche wie die Verarbeitung von sensiblen Kundendaten auszulagern, was zusätzliche Mitarbeiter einspart. Unter diesen Bedingungen kann angenommen werden, dass es hauptsächlich vom Umsatz des Webshops abhängt, ob er zu den KMUs gezählt werden kann.

Abgesehen von den größeren Webshops - ein klassisches Beispiel dafür ist Amazon - gibt es viele kleinere Webshops, die unter die KMU-Definition fallen. Einer der Gründe für die große Anzahl von KMU-Webshops ist der geringe Aufwand, der für die Gründung eines Webshops nötig ist: Es muss keine Verkaufsfläche angemietet werden, alle Produkte werden über das Internet präsentiert. Außerdem werden weniger Mitarbeiter als bei einem klassischen Einzelhandelsgeschäft benötigt. Durch eine extreme Spezialisierung im Warenangebot können sich auch kleinere Mitbewerber auf dem Markt behaupten (S. 68, [16]).

Für die Präsentation der Produkte im Internet muss eine entsprechende Infrastruktur vorhanden sein. Der Aufbau der Webshops wird in Abschnitt 3.1 beschrieben. Diese Infrastruktur muss ständig verfügbar sein, damit Umsatz durch Kundenbestellungen generiert werden kann. Mögliche Gefährdungen werden in Form einer Sicherheitsbetrachtung in Abschnitt 3.2 aufgezeigt: So können nicht nur technische Fehler zu Ausfällen führen, die Verfügbarkeit des Webshops wird vor allem durch Bedrohungen aus dem Internet gefährdet. Des Weiteren muss gewährleistet sein, dass die Daten des Webshops, beispielsweise die Preise für Produkte, nicht unberechtigt verändert werden. Zusätzlich erfordern rechtliche Vorgaben wie die des Bundesdatenschutzgesetzes (siehe Abschnitt 3.2.1), dass die Kundendaten vertraulich behandelt werden. Diese Schutzziele sind in Abschnitt 3.2.2 erläutert. In Abschnitt 3.2.3 werden Gefährdungen für die Schutzziele analysiert und typische Angriffe vorgestellt.

3.1 Aufbau

Die technische Infrastruktur ist unentbehrlich für die Geschäftsprozesse und den Betrieb des Webshops. Sie lässt sich grob in die zwei Komponenten Software und Hardware gliedern: Zur Hardware gehören vor allem die Server, aber auch die Netzwerk-Infrastruktur und die PCs der Mitarbeiter. Die Software beinhaltet zum Beispiel die Shop-Applikation, die die Webseiten mit den Produkten generiert. Außerdem existiert eine Bezahl-Schnittstelle (siehe Abschnitt 3.1.3), die auch als Software realisiert ist und die Verbindung zwischen dem Webshop und den Bezahl-System-Anbietern darstellt. Diese Komponente ist sicherheitskritisch und muss vor allem untersucht werden, wenn sie vom Webshop selbst implementiert wurde. Für die gängige Shop-Software gibt es vorgefertigte Bezahl-Schnittstellen. Die Bezahl-Systeme

(siehe Abschnitt 3.1.4) befinden sich in der Regel außerhalb des Einflussbereichs des Webshops. Aufgrund der Vielfalt der existierenden Webshops ist es schwierig, einen allgemeinen Aufbau zu beschreiben. Die Abbildung 3.1.1 versucht, einen Überblick über die wichtigsten Komponenten eines Webshops (die in den Abschnitten 3.1.1 bis 3.1.4 erklärt werden) zu geben. Software-Komponenten werden durch abgerundete Boxen repräsentiert, die Hardware wurde zu einer Komponente zusammengefasst. Das Betriebssystem bildet die Basis für die weitere Software, die Webserver-Komponente ist eine Software, die für die Veröffentlichung der Webseite im Internet benötigt wird. Beide Komponenten sind nicht Webshop-spezifisch und werden daher nicht weiter erläutert. Neben der vorhandenen Schnittstelle zu Banken und Bezahlssystemen wäre auch eine Anbindung an ein Enterprise-Resource-Planning-System¹ oder zu Logistikunternehmen denkbar.

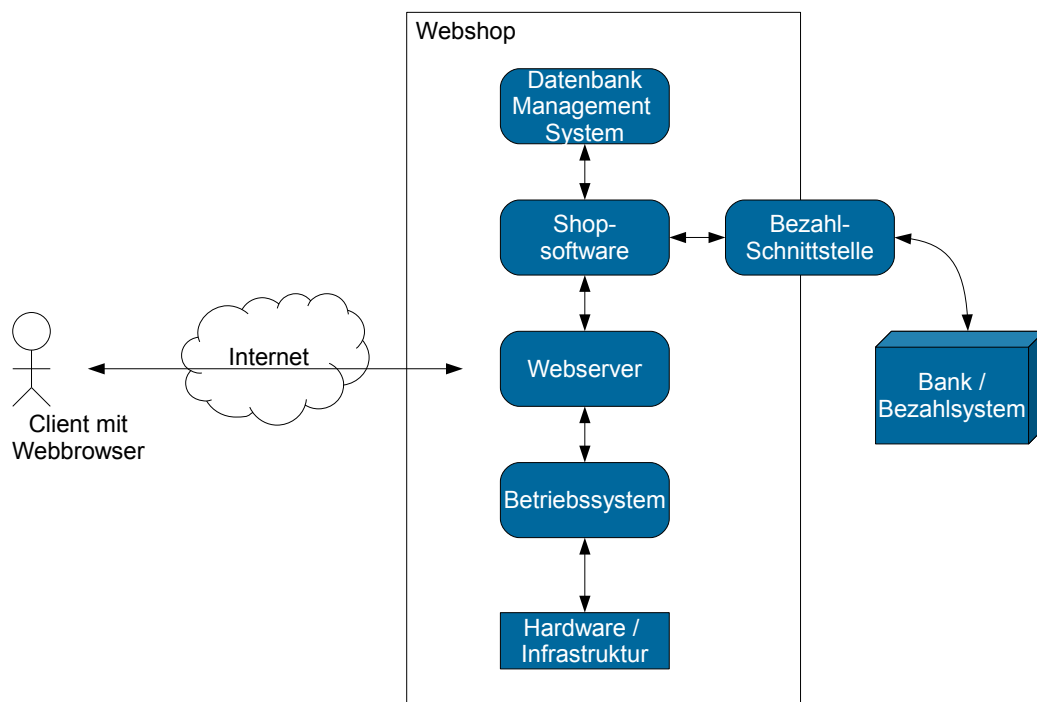


Abbildung 3.1.1: Schematische Darstellung des Aufbaus eines Webshops²

Ein Webshop kann die gesamte technische Infrastruktur und deren Wartung auslagern, in dem Fall liegt die Sicherheit zu großen Teilen nicht mehr in der Verantwortung des Webshops. Dieser beteiligt sich dann hauptsächlich redaktionell durch das Einstellen der Inhalte am Web-Auftritt. Diese Möglichkeit ist für die weitere Betrachtung weniger interessant, da hier kaum Einfluss auf die Gestaltung der Sicherheit genommen werden kann und die in den folgenden Kapiteln beschriebenen Methoden nicht anwendbar sind. Natürlich sollte in diesem Fall sichergestellt werden, dass der mit der Auslagerung beauftragte Dienstleister für die Sicherheit der Daten und der Infrastruktur sorgt. In dieser Arbeit liegt der Fokus auf Webshops, die keine Infrastruktur ausgelagert haben und daher für die Evaluation und Verbesserung der Sicherheit selbst verantwortlich sind.

¹ Eine Software zur Planung der Unternehmensressourcen wie Personal oder Betriebsmitteln - zum Beispiel könnte so die noch vorhandene Stückzahl eines Artikels bestimmt und im Webshop angezeigt werden.

² Teilweise übernommen von <http://www.at-mix.de/ecommerce/online-shops-020101.htm>, aufgerufen am 18.08.2010

3.1.1 Hardware

Die Hardware von Webshops variiert je nach Größe und Outsourcing-Anteil. Bei kleineren Webshops befinden sich alle Anwendungen auf einem einzelnen Server, größere Webshops besitzen entsprechend eine größere Anzahl an Servern sowie Komponenten, die die Kundenanfragen unter ihnen aufteilen³. Ein Webshop mit mehreren Servern könnte beispielsweise folgende Komponenten besitzen (vgl. [32], Seite 39):

- Ein **Server** mit Zugang zum Internet, der Kundenanfragen empfängt, weiterleitet und beantwortet. Er kann als Verbindung zwischen dem Internet und dem lokalen Netz mit den Anwendungs- und Datenservern dienen.
- Ein **Anwendungsserver** auf dem die benötigte Software (siehe Abschnitt 3.1.2) installiert ist.
- Ein **Datenbankserver**, welcher Produktinformationen, Kundendaten und Transaktionen in einer Datenbank speichert.
- Netzwerk-Infrastruktur für die Verbindung zum Internet, zum Beispiel Router und Netzkabel.
- Ein PC zum Verwalten der Shop-Software (für administrative Aufgaben wie dem Hinzufügen von neuen Produkten zum Webshop)

Die Liste ist nicht erschöpfend, optionale Komponenten sind unter anderem Backup-Systeme oder Hardware zur Verteilung der Serverlast. Zur besseren Absicherung des Webshops kann auch eine Hardware-Firewall eingesetzt werden.

3.1.2 Software

Die Software bestimmt maßgeblich die Funktionen des Webshops. Die wichtigste Komponente ist die eigentliche Shop-Software, die das Präsentationssystem enthält, welches für die Darstellung der Produkte und Gestaltung der Webseite verantwortlich ist. Eine Datenbank zur Speicherung der Produkte, Kunden- und Verwaltungsdaten ist entweder schon in die Software integriert oder wird zusätzlich benötigt. In den Abbildungen 3.1.1 und 3.1.2 wird sie in der Komponente „Datenbank Management System“ berücksichtigt.

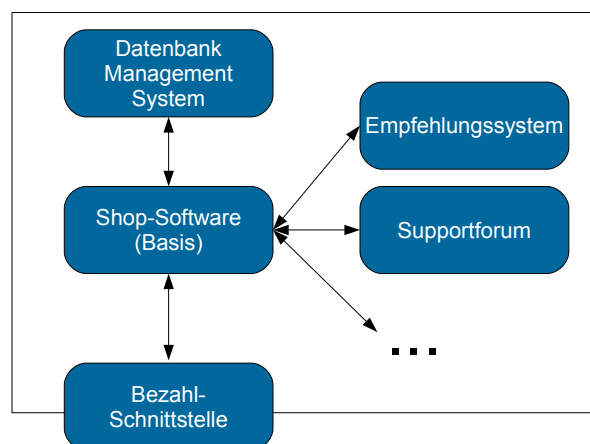


Abbildung 3.1.2: Schematische Darstellung der Shop-Software mit zusätzlichen Modulen

³ In Abbildung 3.1.1 werden beide Fälle durch die Komponente „Hardware/Infrastruktur“ abgedeckt.

Des Weiteren wird zusätzliche Software, die mit der Shop-Software interagiert, eingesetzt, meist in Form von Modulen, die die Hersteller der Shop-Software anbieten (siehe Abbildung 3.1.2). Typische Funktionen sind Empfehlungsdienste (recommendation engine), die anhand der betrachteten und gekauften Artikel eines Kunden Vorschläge generieren und Programme, welche das Kaufverhalten der Nutzer analysieren und daraus Statistiken erstellen. Auch Webshops nutzen die „Web2.0“-Bewegung und integrieren kollaborative und interaktive Elemente, beispielsweise ein Supportforum oder eine Integration von sozialen Netzwerken. Auf die Bezahl-Schnittstelle wird in Abschnitt 3.1.3 näher eingegangen.

Viele Webshops verwenden vorgefertigte Shop-Software, statt eigene zu entwickeln. Neben Open-Source Software gibt es zwei verschiedene Vertriebsmodelle: Entweder wird die Software für einen einmalig zu zahlenden Betrag verkauft oder es wird ein Mietvertrag geschlossen, der monatliche oder jährliche Zahlungen beinhaltet. Oft wird hierbei nicht nur die Software, sondern auch die Hardware vermietet.

Produkt	Trusted Shops vorzertifiziert ⁴	SSL	Preis	andere Sicherheitseigenschaften
cosmoshop	ja	ja	150 € + 79 €/Monat oder 795 € einmalig	
epages	ja	ja	ab 9 €/Monat	
Gambio GX	ja	ja	149 €	
Magento	ja	ja	Freeware bzw. ab 2995 \$/Jahr	Anleitung, wie Magento zur PCI-Compliance konfiguriert werden muss (speichert keine Kartendaten)
oxid eshop 4	ja	ja	Freeware bzw. ab 1990 €	
Smartstore.biz	ja	?	ab 199 €	
STRATO Shops	ja	ja	ab 9,90 €/Monat	TüV zertifizierte Rechenzentren (nach ISO 27001)
WEBSALE eCommerce	ja	ja	ab 69 €	PCI-zertifiziert, Tripple-DES-Verschlüsselung der gespeicherten Bestellungen, TüV SÜD/EHI vorzertifiziert
xt:commerce	ja	ja	ab 97 €	

Tabelle 3.1: Auflistung einiger gängiger Verkaufsportale und ihrer Sicherheitseigenschaften⁵

Durch eine Untersuchung der am häufigsten benutzten Shop-Software kann festgestellt werden, ob die Software bereits Maßnahmen gegen Angriffe enthält. Die Tabelle 3.1 listet einige Produkte auf und beschreibt Sicherheitsfunktionen, die den Webseiten der Hersteller entnommen wurden. Auffällig ist, dass alle größeren Anbieter eine Kooperation mit dem Gütesiegelanbieter Trusted Shops eingehen und ihre Software vorab prüfen lassen. Dies ermöglicht den Webshops, die die Software benutzen, günstigere Konditionen bei der Zertifizierung, da nicht mehr die Software selbst, sondern nur noch die Inhalte (zum Beispiel AGB, Impressum) und organisatorische Prozesse überprüft werden müssen. SSL ist als sicheres Protokoll für die Übertragung von Kundendaten etabliert und wird von nahezu allen Shops verwendet. Darüber hinaus sind nicht viele sicherheitsrelevante Informationen über die Angebote zu erfahren.

3.1.3 Bezahl-Schnittstelle

Neben der eigenständigen Entwicklung und Betreuung der Schnittstelle zwischen dem Webshop und den Banken und Bezahlssystemen bietet sich die Möglichkeit, ein vorgefertigtes Modul des Herstellers

⁴ Siehe Abschnitt 5.1.1.

⁵ Quelle: jeweilige Herstellerhomepages und die Trusted Shops Webseite (<http://www.trustedshops.de/shopbetreiber/shoploesungen.html> , aufgerufen am 05.08.2010).

der Shop-Software zu verwenden oder einen Dienstleister (Payment-Service-Provider) mit der Zahlungsabwicklung zu beauftragen. Bei letzterem wird sowohl der Aufwand für die Pflege der Zahlungssysteme als auch die damit verbundenen Sicherheitsanforderungen an den Provider abgegeben. Dies hilft zum Beispiel, wenn Kreditkarten als Zahlungsmittel angeboten werden, da hier die Anforderungen eines Standards (PCI-Standard, siehe Abschnitt 4.3) eingehalten werden müssen. Vor allem wenn viele Zahlungsmöglichkeiten angeboten werden, steigen die Kosten und der Aufwand für die Verwaltung der verschiedenen Zahlungssysteme. Bei der Verwendung eines Payment-Service-Providers (PSP) muss nur eine Schnittstelle gepflegt werden, die alle vom PSP angebotenen Zahlungssysteme unterstützt. Beim Einsatz von Standard-Shop-Software (Beispiele sind in Tabelle 3.1 aufgelistet) sind Module für verschiedene Bezahlssysteme bereits integriert oder werden zusätzlich angeboten (die Software xt:commerce enthält beispielsweise schon die Bezahlung per PayPal⁶).

3.1.4 Bezahlssysteme

Webshops bieten außer traditionellen Möglichkeiten der Bezahlung wie Vorkasse, Rechnung, Kreditkarte und Nachname in der Regel auch die Zahlung mit sogenannten Bezahlssystemen (siehe Abbildung 3.1.3 für Beispiele) an, die sich auf den Transfer von Geld im Internet spezialisiert haben und eine unkomplizierte Nutzung und größere Sicherheit versprechen.

Von Vorteil ist dabei, dass Kunde und Webshop nach der Transaktion keine Bankdaten des Geschäftspartners kennen. Bei einigen Diensten sind zusätzliche Absicherungen implementiert - beispielsweise erhält der Käufer bei PayPal den Kaufpreis zurück, wenn die Ware nicht verschickt wurde⁷. Eine Einbindung dieser Systeme dient also der Kundenzufriedenheit, durch die Einbindung mehrerer Anbieter können potenziell mehr Kunden erreicht werden. Da dies mit einigem Aufwand verbunden ist, kann - wie in Abschnitt 3.1.3 beschrieben - ein externer Dienstleister damit beauftragt werden.

Für die technische Sicherheit des Webshops muss lediglich die Schnittstelle betrachtet werden, die Bezahlssysteme an sich sind jedoch irrelevant, sodass hier keine weitere Vertiefung des Themas erfolgt.



Abbildung 3.1.3: Beispiele für Online-Bezahlssysteme⁸

3.2 Sicherheitsbetrachtung

In diesem Abschnitt soll eine allgemeine Sicherheitsbetrachtung von Webshops stattfinden. Da kein konkreter Webshop vorliegt, können keine Schwachstellen analysiert werden. Im Folgenden werden daher

⁶ <http://www.xt-commerce.com/de/Funktionsliste> , aufgerufen am 14.10.2010.

⁷ <https://www.paypal-deutschland.de/sicherheit/schutzprogramme/kauferschutz.html> , aufgerufen am 14.10.2010

⁸ http://business.chip.de/artikel/Online-Bezahlssystem-im-ueberblick_39733071.html, aufgerufen am 18.08.2010.

zunächst rechtliche Anforderungen und Schutzziele untersucht und danach die Gefährdungen analysiert. Mit dieser Grundlage können die vorgeschlagenen Sicherungsmaßnahmen in der Analyse (siehe Kapitel 7) bewertet werden.

3.2.1 Rechtliche Anforderungen

Ein Webshop muss viele rechtliche Formalitäten beachten, vor allem zu den Allgemeinen Geschäftsbedingungen und dem Widerrufsrecht. Für die IT-Sicherheit gibt es kein einheitliches Gesetz [35]. Von Bedeutung sind vor allem die Vorgaben des Bundesdatenschutzgesetzes (BDSG)⁹, die alle Unternehmen, die Kundendaten speichern, nutzen oder verarbeiten, einhalten müssen. Dort wird definiert, wie die Daten zu behandeln sind und zu welchen Zweck sie eingesetzt werden dürfen. In Bezug auf die technische Absicherung ist §9 relevant, welcher beschreibt, dass mittels technischer und organisatorischer Maßnahmen die in dem Gesetz beschriebenen Vorschriften eingehalten werden sollen. In einer Anlage zu dem Gesetzestext sind die Anforderungen an die Maßnahmen aufgelistet, die zur Erfüllung des Datenschutzes notwendig sind (siehe Abbildung 3.2.1). In §9a wird ein Datenschutzaudit thematisiert, der die Möglichkeit einer unabhängigen Prüfung des Datenschutzes bietet. Die zugelassenen Gutachter bewerten dabei sowohl das Konzept als auch technische Einrichtungen und veröffentlichen das Ergebnis. Näheres sollte in einem eigenen Gesetz geregelt werden, welches jedoch nicht verabschiedet wurde. Von organisatorischer Seite verlangt §5 des BDSG, dass die Mitarbeiter zum Datenschutz verpflichtet werden.

Neben dem Bundesdatenschutzgesetz ist das Telemediengesetz¹⁰ für den Datenschutz von Bedeutung. Dort finden sich allerdings keine sicherheitsrelevanten Anforderungen.

- | | |
|----|---|
| 1. | Unbefugten wird physischer Zutritt zu Datenverarbeitungsanlagen verwehrt (Zutrittskontrolle) |
| 2. | Nutzung von Datenverarbeitungssystemen durch Unbefugte wird verhindert (Zugangskontrolle) |
| 3. | Berechtigte Benutzer können ausschließlich auf Daten zugreifen, die ihrer Zugriffsberechtigung unterliegen. Personenbezogene Daten werden während der Verarbeitung und nach der Speicherung nicht unbefugt gelesen oder manipuliert (Zugriffskontrolle) |
| 4. | Personenbezogene Daten können während der Übertragung nicht unbefugt gelesen oder manipuliert werden. Die Übermittlung personenbezogener Daten kann nachvollzogen werden (Weitergabekontrolle) |
| 5. | Die Eingabe von und Manipulation an personenbezogenen Daten ist im Nachhinein nachvollziehbar (Eingabekontrolle) |
| 6. | Personenbezogene Daten werden nur entsprechend den Anweisungen des Auftraggebers (sofern vorhanden) verarbeitet (Auftragskontrolle) |
| 7. | Personenbezogene Daten sind gegen Verlust und zufällige Zerstörung geschützt (Verfügbarkeitskontrolle) |
| 8. | Zu unterschiedlichen Zwecken erhobene Daten können getrennt verarbeitet werden |

Abbildung 3.2.1: Die Kontrollen aus der Anlage zu §9 Satz 1 des BDSG

Des Weiteren kann das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) Auswirkungen auf Webshops haben. Dieses Artikelgesetz betrifft hauptsächlich Aktiengesellschaften. Es fordert die Einführung eines Überwachungssystems, das die Erkennung, Bewertung und Behandlung von Risiken enthält (siehe Aktiengesetz §91 (2)). Der genaue Wirkungsbereich ist im Gesetz nicht weiter

⁹ http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf , aufgerufen am 12.10.2010.

¹⁰ <http://www.gesetze-im-internet.de/bundesrecht/tmg/gesamt.pdf> , aufgerufen am 12.10.2010.

festgehalten, jedoch ist die IT-Infrastruktur nicht explizit davon ausgenommen. Bei Nichteinhaltung des Gesetzes können Vorstand, Aufsichtsrat und Geschäftsführer für Schäden haftbar gemacht werden. Eine Haftbarkeit der Geschäftsführer ist aber auch bei GmbHs gegeben (siehe Gesetz betreffend die Gesellschaften mit beschränkter Haftung §43).

Neben den genannten rechtlichen Anforderungen kann es vertragliche Vereinbarungen, wie beispielsweise bei der Verarbeitung von Kreditkartendaten geben, die bei der Betrachtung eines konkreten Unternehmens ebenfalls berücksichtigt werden müssen.

3.2.2 Schutzziele

Neben den „klassischen“ Schutzzielen der Informationssicherheit Vertraulichkeit, Verfügbarkeit und Integrität sind Authentizität und Verbindlichkeit für Webshops von Bedeutung.

Vertraulichkeit ist für Kunden- und Transaktionsdaten wichtig. Die Kundendaten müssen sowohl während der Übertragung als auch nach der Speicherung vor unberechtigtem Zugriff geschützt werden.

Verfügbarkeit ist eine wesentliche Anforderung an Webshops. Die Verfügbarkeit der Webseite, des Produktangebots und der Zahlungsmechanismen muss zu jedem Zeitpunkt gewährleistet sein, da sonst kein Umsatz erzielt werden kann.

Die **Integrität** der Webseite und des Angebots muss erhalten bleiben. Eine Veränderung der Produktinformationen durch Unberechtigte muss vermieden werden. Kritisch sind auch die Transaktionsdaten beim Einkaufsvorgang, deren Veränderungen bewirken können, dass ein erworbenes Produkt nicht zugestellt oder der Verkaufspreis nicht eingefordert werden kann.

Die **Authentizität** ist für den Einkaufsvorgang relevant: Der Webshop muss die Daten des Käufers kennen, um das Produkt zu versenden und das Geld einzufordern. Es sollte nicht möglich sein, dass sich eine Person für eine Andere ausgibt¹¹.

Die **Verbindlichkeit** erfordert, dass eine durchgeführte Handlung, etwa eine Bestellung, nicht abgestritten werden kann. Diese Anforderung betrifft den Bestellvorgang und ist mit der Gewährleistung der Authentizität verknüpft.

3.2.3 Gefährdungen

Bei einem komplexen System wie einem Webshop gibt es sehr viele, zum Teil von den Komponenten abhängige Gefährdungen. Um einen Eindruck davon zu bekommen, werden hier Angriffsbäume [36] für die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität vorgestellt. Sie erheben keinen Anspruch auf Vollständigkeit: Um diese ansatzweise zu erreichen, ist eine aufwändigere Risikoanalyse vonnöten.

Es gibt unterschiedliche Gefährdungen für die Infrastruktur des Unternehmens, der Schwerpunkt soll hier aber auf den Gefährdungen durch Angriffen von außen liegen. Dennoch sollte man nicht vergessen, dass bei allen Infrastrukturkomponenten die Gefahr eines technischen Defekts, zum Beispiel aufgrund ihres Alters oder durch Umwelteinflüsse, besteht. Die in den Angriffsbäumen verwendeten Angriffsmethoden (siehe Abbildungen 3.2.2, 3.2.3 und 3.2.4) orientieren sich vor allem an einer Top 10 Liste der kritischen Sicherheitsrisiken von Web-Applikationen [34], die nach der Vorstellung der Angriffsbäume beschrieben wird. Zur besseren Nachvollziehbarkeit wurden in die Angriffsbäume dabei die Bezeichnung der Schwachstellen eingesetzt, obwohl es sich genau genommen um die Angriffe gegen diese Schwachstellen handelt. Statt Angriffsbäume für Schutzziele zu erstellen, wäre es auch möglich gewesen, zwischen Angriffen auf die unterschiedlichen Komponenten des Webshops zu unterscheiden.

¹¹ Bei Webshops, die vom Benutzer keine eindeutige Identifizierung verlangen, ist es Angreifern möglich, sich als eine andere oder sogar nicht-existente Person auszugeben. Durch die Einschränkung der Zahlungsarten wird zumindest verhindert, dass dem Webshop dadurch ein finanzieller Schaden entsteht.

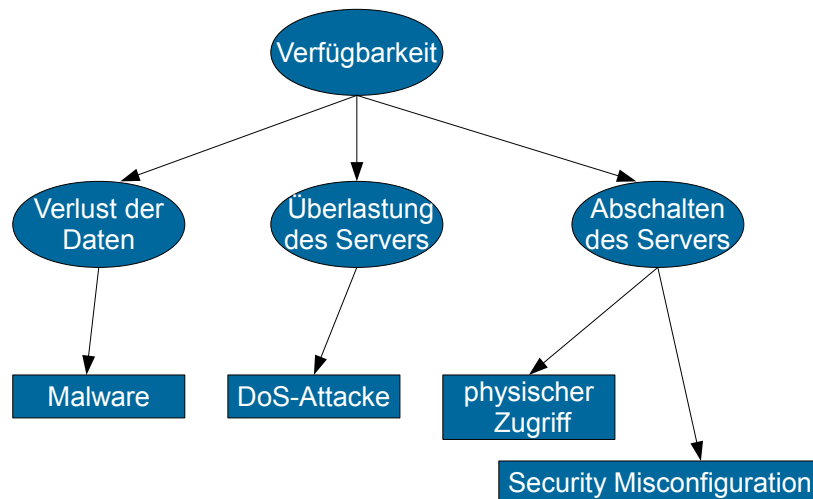


Abbildung 3.2.2: Angriffsbaum zur Verfügbarkeit

Abbildung 3.2.2 gibt einen Überblick über mögliche Angriffe gegen die Verfügbarkeit. Es ist zu beachten, dass die Angriffe meist noch konkreter unterschieden werden. Malware umfasst beispielsweise Spyware, trojanische Pferde, Viren, Würmer und Rootkits. Ein Angriff kann auch mehrere Schutzziele gefährden: Wenn ein Angreifer physischen Zugriff auf den Server hat, kann er ihn ausschalten, Daten auslesen oder verändern. Dies hat eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität zur Folge. Bei einem DoS-Angriff sendet ein Angreifer sehr viele Anfragen an einen Server, sodass dieser nicht mehr auf (andere) Anfragen reagieren kann (denial of service) - beispielsweise weil die Kapazität seiner Netzwerkverbindung oder die Rechenleistung erschöpft ist. Eine Variante davon ist der DDoS-Angriff (distributed denial of service), bei dem sehr viele Clients - meist ferngesteuerte Botnetze - Anfragen an einen Server senden (siehe [10]). Alle anderen Angriffe werden im Zuge der Vorstellung der kritischsten Sicherheitslücken von Web-Applikationen erklärt.

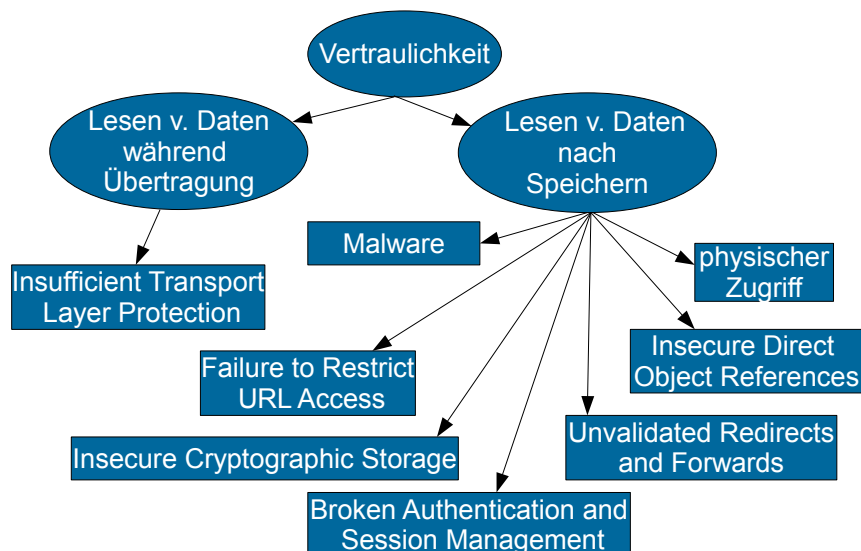


Abbildung 3.2.3: Angriffsbaum zur Vertraulichkeit

Abbildung 3.2.3 zeigt Angriffe gegen die Vertraulichkeit. Das Lesen der Daten während der Übertragung ist nur möglich, wenn letztere ungesichert stattfindet. Wie in Abschnitt 3.1.2 dargestellt, werden die Kundendaten jedoch oft mit Hilfe des SSL-Protokolls (also verschlüsselt) übertragen.

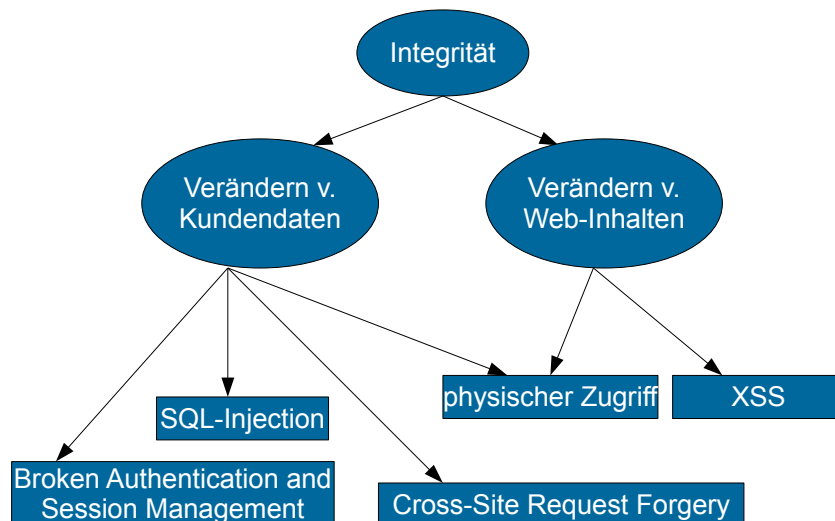


Abbildung 3.2.4: Angriffsbaum zur Integrität

Abbildung 3.2.4 stellt Angriffe gegen die Integrität dar. Im Szenario wird davon ausgegangen, dass die Kundendaten in einer Datenbank gespeichert sind, sodass eine SQL-Injection möglich ist.

Je nach Aufbau der Webseiten und der dahinter liegenden Software sind sehr unterschiedliche Angriffe möglich. Allgemein können Angreifer versuchen, sich Zugang zum Administrationsbereich der Shop-Software zu verschaffen, indem sie die Zugangsdaten raten oder Kontakt mit den Mitarbeitern, beispielsweise dem Administrator, aufnehmen („Social-Engineering“-Angriff). Besonders die Kombination von Angriffen kann effektiv sein.

Eine wichtige Informationsquelle für Webshops ist die in unregelmäßigen Abständen erscheinende Top 10 Liste der kritischen Sicherheitsrisiken von Web-Applikationen des Open Web Application Security Project (OWASP)[34]. Die Top 10 Sicherheitsrisiken wurden in den Angriffsbäumen (siehe Abbildungen 3.2.2, 3.2.3 und 3.2.4) benutzt¹² und werden in der folgenden, nach Rang geordneten Auflistung näher erklärt:

- **Injections** befinden sich auf dem ersten Platz der OWASP-Liste. Ein besonders oft auftretender Angriff ist die *SQL-Injection*: Über eine ungefilterte Nutzereingabe, die in einem Datenbank-Befehl verwendet wird, bekommt der Angreifer Zugriff auf die Datenbank und kann seinerseits Befehle ausführen. Das ist möglich, da die gewählte Eingabe nicht auf SQL-spezifische Kontrollzeichen überprüft wird und dadurch den ursprünglichen Datenbankbefehl verändert oder weitere Befehle hinzufügt (siehe [15]).
- **Cross-Site Scripting (XSS)**: Inhalte einer Webseite werden ausgetauscht oder schädlicher Programmcode ausgeführt, meist mit dem Ziel, an Daten zu gelangen oder Sitzungen zu übernehmen. XSS-Angriffe nutzen aus, dass Benutzereingaben ungefiltert verarbeitet werden. So kann beispielsweise bei einer Such-Funktion, die oft in Webshops enthalten ist, ein böartiges Skript als Suchparameter übergeben werden. Wird dieses der Übersicht wegen nochmals in die HTML-Seite eingebettet, so kann es zur Ausführung des Skripts kommen. Der Angreifer kann nun einen entsprechend vorbereiteten Link zu der Suchanfrage einem anderen Benutzer zukommen lassen, um auf dessen Rechner den Code auszuführen. Andere Szenarien finden sich in [5].
- **Broken Authentication and Session Management** verursacht Schwachstellen durch Fehler in der Programmierung oder ungenügende Schutzmaßnahmen. Angreifer können dies nutzen, um eine

¹² Die Schwachstellen können - je nach Umgebung, in der sie auftreten - auch noch weitere Schutzziele gefährden.

Sitzung an einen Benutzer weiterzugeben und sie nach dessen Anmeldung wieder zu übernehmen (Session-Fixation [27]) oder eine Session-ID zu erraten (Session-Hijacking).

- **Insecure Direct Object References:** Wenn der Zugriff auf interne Objekte nicht geschützt ist, können Angreifer unautorisiert auf Daten zugreifen.
- **Cross-Site Request Forgery:** Ein Angreifer stellt über einen anderen Benutzer eine HTTP-Anfrage (mit dessen Session-ID), die als erlaubte Anfrage des Benutzers aufgefasst wird. Durch Zusehen eines präparierten Links oder eingebetteten Codes an einen privilegierten Benutzer kann ein Angreifer Befehle ausführen, die er mit seinem eigenen Benutzerkonto nicht ausführen kann.
- **Security Misconfiguration:** Das ganze System (bei Webshops die Webshop-Software, die Webserver-Software und das Betriebssystem) muss sicher konfiguriert sein, dazu gehören unter anderem das Anpassen der Sicherheitseinstellungen und Software-Updates. Ansonsten können Angreifer bekannte Schwachstellen ausnutzen, um das System zu kompromittieren.
- **Insecure Cryptographic Storage:** Sensitive Daten (zum Beispiel Kreditkarten- und Anmeldedaten) müssen durch angemessene Kryptographie geschützt sein. Unverschlüsselte Daten können von Angreifern gelesen und unzureichende Verschlüsselungen gebrochen werden.
- **Failure to Restrict URL Access:** Berechtigungen müssen nicht nur überprüft werden, wenn Links oder Buttons generiert werden, sondern auch wenn eingeschränkt zugängliche Seiten aufgerufen werden. Angreifer können sonst Seiten direkt aufrufen und so auf vertrauliche Inhalte stoßen.
- **Insufficient Transport Layer Protection:** Sensible Daten, die über ein Netzwerk ausgetauscht werden, müssen durch starke Kryptographie verschlüsselt und mit gültigen Zertifikaten versehen sein. Andernfalls können Angreifer die Kommunikation mitlesen oder verändern.
- **Unvalidated Redirects and Forwards:** Bei der Weiterleitung von Benutzern werden unvertrauenswürdige Daten zur Bestimmung der Zielseiten verwendet. Angreifer können damit unautorisiert Seiten aufrufen oder andere Benutzer zu Malware-Seiten weiterleiten.

4 Standards

Standards der IT-Sicherheit bieten etablierte Lösungswege zur Absicherung der IT an. Gerade für kleinere Unternehmen, die nicht die Ressourcen haben, um eigene, auf sie zugeschnittene Regelwerke zu entwickeln, können sie ein Wegweiser zum Erreichen von IT-Sicherheit sein. Standards können unterteilt werden in Normen, also durch Gremien entwickelte, offizielle Verfahrensweisen sowie allgemein anerkannte und angewendete Regeln (sogenannte Best-Practices).

Die Normengremien bestehen meist aus Mitgliedern der Unternehmen, die auch die Anwender des Standards sind. So ist gewährleistet, dass nicht hohe Kosten für eine Implementierung ausgegeben werden, die ihren Zweck verfehlt. Stattdessen werden bewährte Praktiken aus den Erfahrungen der Teilnehmer gesammelt, die auch für andere Unternehmen hilfreich sind. Gerade bei Normen, die verpflichtend sind, wie beispielsweise der Payment Card Industry Standard bei der Verarbeitung von Kreditkartendaten, kann die Fremdbestimmung durch eine Teilnahme am Gestaltungsprozess der Norm vermindert werden. Meistens bietet sich nach der Anwendung eines Standards eine Möglichkeit, eine Zertifizierung durchzuführen. Diese unabhängige Prüfung schafft Vertrauen und Vergleichbarkeit für Kunden, Mitbewerber und Auftragnehmer. Zertifizierungen können aber auch zusätzliche Kosten und mehr Arbeitsaufwand für Unternehmen bedeuten. Viele der Standards beinhalten jedoch kein starres Regelwerk, sondern lassen einen Interpretationsspielraum zu und sind so auf die Größe des Unternehmens anpassbar. Natürlich können auch Kombinationen von Normen sinnvoll sein, aber gerade KMUs sollten den Aufwand, der für die Umsetzung einer Norm notwendig ist, nicht unterschätzen.

Im Folgenden werden die bekanntesten Standards der IT-Sicherheit beschrieben. Dabei wird besonders darauf eingegangen, inwiefern bei der Anwendung des Standards eine Evaluation der IT-Sicherheit stattfindet. Außerdem wird darauf hingewiesen, ob sie für KMUs allgemein und insbesondere für Webshops umsetzbar oder zumindest anpassbar sind. Die Auflistung ist nicht vollständig - es gibt noch weitere Normen, die aber weniger verbreitet oder älteren Ursprungs sind. Als Entscheidungshilfe für die Auswahl wurde der „Kompass der IT-Sicherheitsstandards“ von BITKOM [4] und ein Bericht der Initiative D21 [22] verwendet. Mit Hilfe des in Abschnitt 1.4 vorgestellten Templates werden die Standards analysiert. Zunächst werden die beiden Standards für Informationssicherheits-Managementsysteme, ISO 27001 und IT-Grundschutz vorgestellt, danach folgen der bei der Verarbeitung von Kreditkarten zu berücksichtigende Payment Card Industry Data Security Standard, das risiko-orientierte OCTAVE, der auf IT-Servicemanagement fokussierte ITIL-Standard, das IT-Governance-Framework Cobit, der Wirtschaftsprüfer-Standard IDW PS 330 und schließlich die Common Criteria.

4.1 ISO/IEC 27001

Die ISO/IEC 27001 Norm beschreibt Anforderungen an ein Managementsystem für Informationssicherheit (ISMS), welches Richtlinien und Verfahren beinhaltet, um Informationssicherheit systematisch auf allen Ebenen des Unternehmens zu etablieren und zu erhalten. Sie ist aus dem British Standard 7799 entstanden und wurde 2005 veröffentlicht. Wie andere ISO/IEC-Normen ist sie in eine Normenfamilie eingegliedert (siehe Tabelle 4.1). In ISO 27002 werden beispielsweise die Ziele der benötigten Maßnahmen beschrieben, die Norm ist aufgeteilt in elf Bereiche (siehe Abbildung 4.1.1), 39 Kontrollziele und 133 Sicherheitsanforderungen. Sie ist mit anderen ISO/IEC-Normen wie ISO 9000 (Qualitätsmanagement) kompatibel und kann in ein allgemeineres Managementsystem eingebunden werden.

ISO 27001 ist international anerkannt: Weltweit wurden 6573 Zertifizierungen durchgeführt, in Deutschland 138¹. Die Norm beschreibt den Aufbau und Betrieb eines ISMS und orientiert sich am sogenannten Plan-Do-Check-Act-Zyklus (siehe Abbildung 4.1.2). Sie ist auf eine kontinuierliche Verbesserung des ISMS ausgelegt.

¹ <http://www.iso27001certificates.com/Register%20Search.htm> , aufgerufen am 04.08.2010.

Bezeichnung	Inhalt
27000	Einführung/Überblick, Glossar der Begrifflichkeiten
27001	Anforderung an das ISMS (gegen die zertifiziert wird), 11 Themengebiete von Schutzziele
27002	Code of Practice, enthält Maßnahmenpakete (+ Erläuterungen und Hinweise)
27003	Anweisungen zur Implementierung
27004	Standard zur Messung des Managementsystems
27005	Standard für Risikomanagement

Tabelle 4.1: Die ISO 27000-Normenfamilie

In der Plan-Phase legen die Verantwortlichen, in der Regel das Management des Unternehmens, den Anwendungsbereich des ISMS fest und definieren eine ISMS- und Informationssicherheitsrichtlinie, die alle Anforderungen und Rahmenbedingungen an das ISMS enthält. Ein wichtiger Bestandteil der Norm ist die Risikoanalyse, sie kann beispielsweise mit ISO 27005 durchgeführt werden und folgt dann ebenfalls dem PDCA-Zyklus. Da die Norm keine Vorgaben macht, ist jede andere Methode ebenfalls möglich, so können die Verantwortlichen eines kleineren Unternehmens auch eine einfache Risikomatrix [2] als Risikoabschätzung wählen. Es muss lediglich gewährleistet sein, dass Bedrohungen und Schwachstellen analysiert und eine Abschätzung und Bewertung der Risiken vorgenommen wird, sodass schließlich eine priorisierte Liste von Risiken vorhanden ist. Für diese Risiken müssen nun Maßnahmen ausgewählt werden. Die Ziele dieser Maßnahmen können ISO 27002 entnommen werden, die Suche und Auswahl geeigneter Maßnahmen muss allerdings eigenständig durchgeführt werden. Die Risiken und ausgewählten Maßnahmen müssen durch das Management bestätigt und in der Erklärung zur Anwendbarkeit (statement of applicability) festgehalten werden. Bei späteren Iterationen werden in der Plan-Phase die Dokumente und ausgewählten Methoden anhand der Ergebnisse aus den vorigen Phasen angepasst.

- | | |
|-----|--|
| 1. | Sicherheitsleitlinie |
| 2. | Organisation der Informationssicherheit |
| 3. | Management von organisationseigenen Werten |
| 4. | Personalsicherheit |
| 5. | Physische und umgebungsbezogene Sicherheit |
| 6. | Betriebs- und Kommunikationsmanagement |
| 7. | Zugangskontrolle |
| 8. | Beschaffung, Entwicklung und Wartung von Informationssystemen |
| 9. | Umgang mit Informationssicherheitsvorfällen |
| 10. | Sicherstellen des Geschäftsbetriebs (Business Continuity Management) |
| 11. | Einhaltung von Vorgaben (Compliance) |

Abbildung 4.1.1: Die Bereiche der ISO 27002 Norm²

² <http://www.beuth.de/?workflowname=infoInstantdownload&docname=1463759&ixos=toc>, aufgerufen am 29.09.2010.

In der Do-Phase folgt die Implementierung: Die Leitlinie wird angewendet und die beschlossenen Maßnahmen umgesetzt. Dazu müssen Ressourcen bereit gestellt und Mitarbeiter geschult werden. Durch interne ISMS-Audits und Management-Reviews wird regelmäßig der aktuelle Stand der Umsetzung gemessen. Dies beinhaltet auch eine Abschätzung der Wirksamkeit der einzelnen Maßnahmen. Während dem Betrieb des ISMS kann es zu Sicherheitsvorfällen kommen. Diese müssen erkannt und behoben werden. Im Standard wird dazu ein Incident Management-Plan empfohlen, der die Klassifizierung der Vorkommnisse und für jede Klasse separate Notfallpläne enthält.

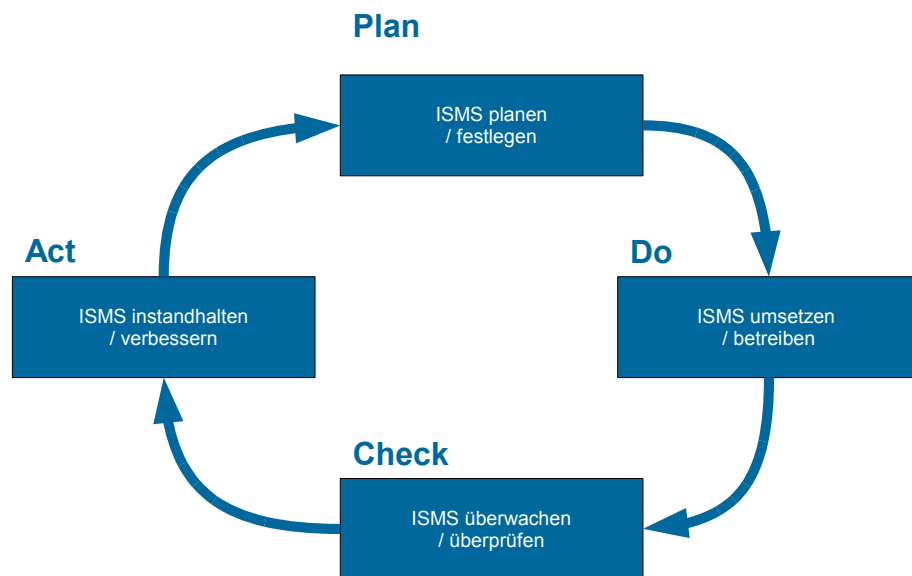


Abbildung 4.1.2: Der PDCA-Zyklus von ISO 27001 (S. 38, [24])

In der Check-Phase wird die Sicherheit gemessen und mit dem Soll-Wert, festgelegt durch die Informationssicherheitsrichtlinie, verglichen. Die Messung erfolgt durch Metriken, die beispielsweise in ISO 27004 definiert sind. Wichtige Indikatoren sind hier die aufgezeichneten Sicherheitsvorfälle und die Ergebnisse der Wirksamkeitsabschätzungen und Management-Reviews.

Die vierte und letzte Phase (Act) führt gegebenenfalls korrigierende Maßnahmen durch, indem sie die identifizierten Verbesserungen umsetzt. Diese werden ebenfalls dokumentiert und überprüft. Danach wird die nächste Plan-Phase vorbereitet.

Nähere Details zu den einzelnen Phasen des PDCA-Zyklus finden sich in [24]. Um die Umsetzung des Standards zu unterstützen, gibt es verschiedene Software-Werkzeuge, unter anderem das kostenlose Tool verinice³.

Ebene

Die Verbesserung der Informationssicherheit wird ausgehend von den Geschäftsprozessen des Unternehmens beschrieben, es handelt sich hierbei also um einen Top-Down-Ansatz. Es werden organisatorische Anforderungen statt konkreter technischer Maßnahmen vorgegeben.

Voraussetzungen

Der Standard stellt keine speziellen Anforderungen an ein Unternehmen, durch seine generische Beschreibungen ist er branchen- und größenunabhängig. Weil keine konkreten Methoden vorgeschrieben werden, müssen Mitarbeiter mit Wissen im Bereich IT-Sicherheit und Risikoanalyse vorhanden sein.

³ <http://v.de> , aufgerufen am 29.09.2010.

Prüfung

Die Prüfung besteht aus mehreren Audits, wobei in einem ersten Schritt nur die Dokumente analysiert werden und danach erst die Einhaltung der Anforderungen überprüft wird⁴. Ein Zertifikat wird für 3 Jahre ausgestellt, es werden jährliche Überprüfungsaudits durchgeführt. Die Zertifizierung erfolgt durch akkreditierte Zertifizierungsstellen (diese können der Webseite der deutschen Akkreditierungsstelle⁵ entnommen werden).

Aufwand und Kosten

Der Aufwand für die Zertifizierung bei KMUs beträgt abhängig von den Rahmenbedingungen vier bis acht Monate [37]. Ausschlaggebend ist unter anderem die bisherige Qualität der Organisation im Unternehmen ([22], S. 24). Der Standard ist kostenpflichtig, die Kosten für die Umsetzung sind abhängig von der Größe des Unternehmens, den bisher getroffenen Maßnahmen und der Erfahrung der Mitarbeiter. Laut einer englischen Webseite⁶ kostet eine Zertifizierung aber mehr als 10.000 Dollar.

Nutzen und Anpassbarkeit

Mit der ISO 27001 Norm kann die IT-Sicherheit nicht nur bewertet, sondern auch systematisch verbessert werden. Für die Evaluation ist die Wahl der Methode für die Risikoanalyse entscheidend, da es von ihr abhängt, ob alle Schwachstellen erkannt werden.

Der Standard ist nicht speziell auf kleine Unternehmen zugeschnitten, aber generisch gehalten und deshalb für verschiedenste Unternehmen, auch für KMU, einsetzbar. Statt konkreter Maßnahmen wird beschrieben, was für die Erstellung, den Betrieb und die Wartung von ISMS notwendig ist, aber dem Unternehmen wird bei der konkreten Implementierung Freiraum gelassen. Daher können die Maßnahmen - je nach Unternehmenssituation - angemessen gewählt werden. Des Weiteren müssen nicht alle Teilbereiche eines Unternehmens zertifiziert werden ([4], S. 18).

Eine Studie untersuchte die Umsetzung der Norm ISO 27001 in deutschen KMUs [25] und kam zu dem Ergebnis, dass 30 der 133 vorgegebenen Maßnahmen aus ISO 27002 in einer typischen KMU nicht anwendbar sind, als Gründe wurden eine schwache Marktposition, technische Schwierigkeiten, fehlendes Wissen/Personal und eine zweifelhafte Kosten-Nutzen-Relation genannt.

4.2 ISO 27001 basierend auf IT-Grundschutz

Der vom Bundesamt für Informationssicherheit (BSI) veröffentlichte Standard IT-Grundschutz sichert die IT-Infrastruktur von Unternehmen mithilfe eines Managementsystems für Informationssicherheit (ISMS) ab. Grundwerte der IT-Sicherheit sind dabei Vertraulichkeit, Verfügbarkeit und Integrität. Der Schutz dieser Werte wird durch Analyse der Infrastruktur mit anschließender Auswahl und Durchführung von vorgegebenen Maßnahmen erreicht.

Das BSI hat 2005 das IT-Grundschutzhandbuch und dessen Zertifizierung überarbeitet. Die ab 2005 vergebenen Zertifikate bescheinigen Konformität zur ISO 27001 basierend auf IT-Grundschutz. Durch Anlehnung an eine internationale ISO-Norm und Veröffentlichung einer englischen Übersetzung des Standards soll die weltweite Anerkennung sichergestellt werden. Im Gegensatz zu ISO 27001 wird dieser Standard aber momentan nicht international eingesetzt. Im Jahr 2004, also vor der Annäherung an ISO 27001, gab es selbst in Deutschland nur fünf zertifizierte Unternehmen, 2010 sind es immerhin 38 Unternehmen und neun laufende Zertifizierungen⁷.

⁴ <http://www.27001-online.com/auditing.htm> , aufgerufen am 04.10.2010.

⁵ http://www.dakks.de/akkreditierte_stellen , aufgerufen am 05.10.2010.

⁶ <http://www.maxi-pedia.com/ISO+27001> , aufgerufen am 29.09.2010.

⁷ https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/zert/veroeffentl/ISO27001Zertifikate/iso27001_zertifikate.html, aufgerufen am 04.08.2010.

Bezeichnung	Inhalt
BSI-Standard 100-1	Managementsysteme für Informationssicherheit (ISMS)
BSI-Standard 100-2	Vorgehensweise nach IT-Grundschutz
BSI-Standard 100-3	Risikoanalyse nach IT-Grundschutz

Tabelle 4.2: Tabelle zu BSI-Standards aus [19]

Der Standard orientiert sich am Plan-Do-Check-Act-Zyklus (PDCA). Wie bei den ISO-Normen ist der Standard in mehrere Teile aufgeteilt (siehe Tabelle 4.2). Zusätzlich werden noch die IT-Grundschutz-Kataloge benötigt, die aus Bausteinen, einem Gefährdungskatalog und einem Maßnahmenkatalog bestehen⁸. Die Abbildung 4.2.1 liefert einen Überblick über die Vorgehensweise, die im Weiteren erläutert wird.

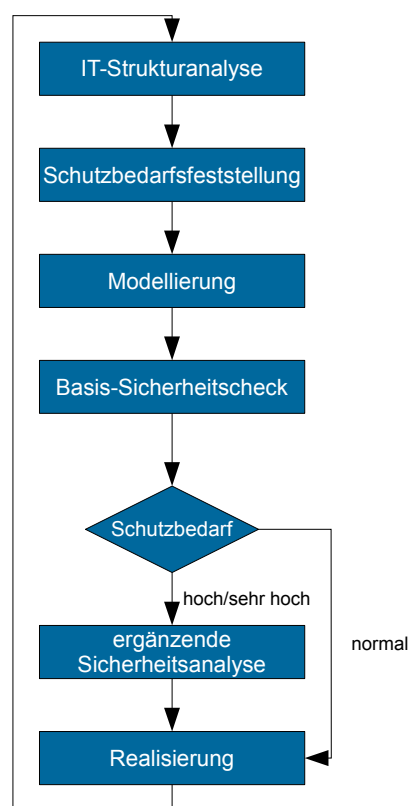


Abbildung 4.2.1: Die Vorgehensweise nach Grundschutz-Methodik

Um ein norm-konformes Managementsystem für Informationssicherheit (ISMS) zu implementieren, muss zunächst der Geltungsbereich festgelegt werden. Die ausgewählten und im weiteren Verlauf betrachteten Komponenten werden als IT-Verbund bezeichnet. Beim IT-Grundschutz handelt es sich dabei vor allem um technische Komponenten wie Server oder Datenleitungen.

Als nächstes werden die Sicherheitsziele, ihr Zusammenhang mit den Geschäftszielen und eine Strategie für ihre Umsetzung definiert. Dabei sollten Rahmenbedingungen wie gesetzliche Vorgaben, von denen das Unternehmen betroffen ist, oder bereits bestehende interne Richtlinien beachtet werden. Alle relevanten Ergebnisse werden in einer IT-Sicherheitsleitlinie festgehalten, die nach ihrer Fertigstellung im Unternehmen veröffentlicht wird, um das Bewusstsein aller Mitarbeiter für IT-Sicherheit

⁸ https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, aufgerufen am 05.10.2010.

zu sensibilisieren. Außerdem muss eine IT-Sicherheitsorganisation aufgebaut werden, die im Wesentlichen aus einem oder mehreren IT-Sicherheitsbeauftragten besteht. Sie sind Ansprechpartner für alle IT-Sicherheits-Themen und organisieren unter anderem den Sicherheitsprozess, führen Sensibilisierungsmaßnahmen durch und untersuchen IT-Sicherheitsvorfälle.

In der darauf folgenden *IT-Strukturanalyse* wird der aktuelle Zustands des Systems analysiert. Dazu werden zunächst alle Komponenten des IT-Verbunds aufgelistet. Eine graphische Übersicht des Netzwerks (Netzplan) hilft, die Vernetzung der Komponenten zu erkennen, dabei können ähnliche Objekte mit der gleichen Aufgabe zusammengefasst werden. Alle Komponenten und auch die IT-Anwendungen und Räume müssen erfasst werden, sodass eine vollständige Datengrundlage entsteht, anhand derer der Schutzbedarf für alle Objekte festgestellt werden kann.

Mit der *Schutzbedarfsfeststellung* wird eine Priorisierung des Schutzbedarfs für die einzelnen Komponenten vorgenommen. Bei dem Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität treten typischerweise ein oder mehrere Schadensszenarien auf. Im BSI-Standard 100-2 werden dazu Beispiele wie Gesetzesverstöße, finanzielle Auswirkungen oder Imageschäden aufgeführt. Die Szenarien müssen analysiert und in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ eingeteilt werden. Die Einordnung sollte so gewählt sein, dass für einen normalen Schutzbedarf Standard-Sicherheitsmaßnahmen ausreichen. Für alle IT-Anwendungen wird nun festgestellt, inwiefern sie von den Schadensszenarien betroffen sind, welche Grundwerte geschützt werden müssen und wie hoch der Schutzbedarf ist. Es muss beachtet werden, dass IT-Anwendungen voneinander abhängen können. Werden die Ergebnisse einer eher unkritischen IT-Anwendung für eine IT-Anwendung mit hohem Schutzbedarf benötigt, muss der Schutzbedarf entsprechend angepasst werden. Der Schutzbedarf für die IT-Systeme kann von den Anwendungen abgeleitet werden, der Schutzbedarf für die Räume wird von den darin enthaltenen IT-Systemen abgeleitet.

Nummer	Schicht
B1	übergreifende Aspekte
B2	Infrastruktur
B3	IT-Systeme
B4	Netze
B5	IT-Anwendungen

Tabelle 4.3: Schichten des IT-Grundschutzmodells aus [19]

Anschließend folgt die *Modellierung*, die Komponenten im IT-Verbund auf vorgegebene Bausteine der IT-Grundschutz-Kataloge abbildet, um so Gefährdungen und Maßnahmen zu ermitteln. Sie erfolgt anhand von fünf Schichten (siehe Tabelle 4.3), die nacheinander abgearbeitet werden. Zunächst werden organisatorische Aspekte, die oft für alle Teile des IT-Verbunds gültig sind, bestimmt. Danach erst werden detailliertere Anweisungen für Räume, Systeme und einzelnen Anwendungen festgelegt. Jeder Baustein hat eine eindeutige Nummer (die mit der Nummer der Schicht beginnt, siehe Tabelle 4.3) und verweist auf eine oder mehrere Gefährdungen aus dem Gefährdungskatalog und eine oder mehrere Maßnahmen aus dem Maßnahmenkatalog. Letztere sind unterteilt in die Stufen A, B, C und Z. Die ersten drei Stufen sind für die Zertifizierung notwendig, Z bezeichnet optionale Maßnahmen.

Danach wird durch einen *Basis-Sicherheitscheck* der bisherige Umsetzungsgrad der Maßnahmen zu den ausgewählten Bausteinen analysiert. Er besteht aus Sichtung der relevanten Dokumente (zum Beispiel Sicherheitsanweisungen) und Durchführung von Interviews. So wird der Umsetzungsstatus jeder Maßnahme überprüft, mögliche Werte sind dabei „ja“, „teilweise“, „nein“ oder „entbehrlich“. Maßnahmen sind entbehrlich, wenn die entsprechenden Gefährdungen schon auf eine andere Weise behandelt werden, gar nicht erst auftreten oder keinen Schaden anrichten können.

Wenn eine Komponente des IT-Verbunds einen hohen oder sehr hohen Schutzbedarf hat, sind die Standard-Sicherheitsmaßnahmen nach IT-Grundschutz eventuell nicht ausreichend. Außerdem können manche Objekte durch Bausteine nicht gut abgebildet werden, zum Beispiel sehr spezielle Hardware.

In diesen Fällen muss mittels einer *ergänzenden Sicherheitsanalyse* geprüft werden, ob weitergehende Sicherheitsmaßnahmen erforderlich sind, beispielsweise durch eine Risikoanalyse. Dafür gibt es verschiedene Ansätze: Der BSI-Standard 100-3 beschreibt beispielsweise eine Risikoanalyse auf Basis von IT-Grundschutz, die zunächst alle Gefährdungen, welche sich schon aus dem IT-Grundschutz ergeben, auflistet und dann zusätzliche Gefährdungen, die darüber hinausgehen, ermittelt. Für jede Komponente des IT-Verbunds und jede neu entdeckte Gefährdung wird nun überprüft, ob die vorgesehenen Maßnahmen einen ausreichenden Schutz (S. 130 [19]) bieten. Nun muss dem Risiko begegnet werden, entweder durch entsprechende Maßnahmen oder durch Vermeidung, Verlagerung oder Akzeptanz der Risiken. Zur *Realisierung* der festgelegten Maßnahmen werden die Ergebnisse des Basis-Sicherheitschecks hinzugezogen: Alle teilweise oder gar nicht umgesetzten Maßnahmen werden herausgesucht und gegebenenfalls an die Organisation angepasst, da die im IT-Grundschutz beschriebenen Maßnahmen eher allgemeingültig formuliert wurden. In einem Realisierungsplan muss für jede Maßnahme ermittelt werden, wer für die Umsetzung verantwortlich ist und bis wann sie abgeschlossen sein soll. Es sollte nicht nur die Umsetzung der Maßnahmen überwacht werden, sondern auch die Behandlung der auftretenden IT-Sicherheitsvorfälle dokumentiert werden. Die Maßnahmen und die gesamte IT-Sicherheitsstrategie müssen von Zeit zu Zeit bezüglich Aktualität, Effizienz und Wirksamkeit analysiert werden, damit neue oder veränderte Gefährdungen nicht unbemerkt bleiben. Diese Überprüfungen können durch interne und externe Audits vollzogen werden, wobei darauf zu achten ist, dass die Kontrollen nicht von denjenigen durchgeführt werden, die die Sicherheitsmaßnahmen implementiert haben. Die Resultate der Kontrollen werden dafür verwendet, um eine Verbesserung des IT-Sicherheitsprozesses zu erreichen. Dies kann durch Überarbeitung von der ganzen Strategie oder von einzelnen Maßnahmen erreicht werden. Bei größeren Veränderungen wird dabei erneut eine Planungsphase eingeleitet.

Ebene

Der BSI-Standard ist sowohl organisatorisch als auch technisch ausgerichtet. Die Anweisungen zum Etablieren der Sicherheit gehen über die allgemeine Beschreibung von Schutzziele hinaus, für jedes Objekt im IT-Verbund sind konkrete Gefährdungen und Maßnahmen definiert. Insgesamt wird sehr genau beschrieben, wie die IT-Sicherheit zu etablieren ist, sodass der Anwender wenig Wahlmöglichkeiten hat.

Voraussetzungen

Ein wesentlicher Teil des Standards ist nicht anwendbar, wenn die Hardware nicht in den vorgegebenen Bausteinen aufgeführt ist. Dann wird zusätzlicher Aufwand und zusätzliches Wissen benötigt. Damit schwindet der „Vorteil“ gegenüber ISO 27001, bei deren Implementierung Expertenwissen benötigt wird.

Prüfung

Die Evaluation erfolgt durch vom BSI lizenzierte Auditoren⁹ und umfasst die Analyse der erstellten Dokumente, eine Überprüfung der Sicherheitsmaßnahmen vor Ort und die Erstellung eines Audit-Reports, der dem BSI vorgelegt wird. Dieses entscheidet daraufhin, ob ein Zertifikat ausgestellt wird. Die Zertifizierung beinhaltet eine offizielle Zertifizierung nach ISO 27001. Ein Zertifikat ist zwei Jahre gültig, es werden jährliche Überwachungsaudits durchgeführt.

Aufwand und Kosten

Für eine Zertifizierung müssen die ausgewählten Maßnahmen der IT-Grundschutz-Kataloge umgesetzt sein, sofern sie zutreffend und angemessen sind. Es besteht die Möglichkeit, Vorstufen des IT-Grundschutz-Zertifikats zu erlangen. Hierfür muss nur ein Teil der Maßnahmen umgesetzt sein. Das Testat „Einstiegsstufe“ verlangt dabei die Umsetzung aller ausgewählten Maßnahmen, die als Stufe A klassifiziert sind (dies sind die unumgänglichen Standard-Sicherungsmaßnahmen). Entsprechend wird die Erfüllung der wichtigsten Standard-Sicherungsmaßnahmen (Stufe A und B) mit dem Testat „Auf-

⁹ https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Auditoren/iso27001auditoren_node.html, aufgerufen am 05.10.2010.

baustufe“ gekennzeichnet. Für die vollständige Zertifizierung wird auch die Umsetzung der Maßnahmen der Stufe C gefordert. Die Zertifizierung der Vorstufen kosten beim BSI jeweils 45 €, die vollständige Zertifizierung 2.500 €¹⁰. Der größere Teil der Kosten fällt für den Auditor sowie für die Umsetzung der Maßnahmen an.

Der Standard selbst ist frei im Internet verfügbar¹¹. Zur Unterstützung wird vom BSI die kostenpflichtige Software GSTOOL angeboten, es gibt allerdings auch ein kostenloses Werkzeug namens verinice¹².

Nutzen und Anpassbarkeit

Eine erfolgreiche Zertifizierung geht sowohl vom Aufwand als auch vom Nutzen weit über eine Evaluierung der IT-Sicherheit hinaus, da der Standard auf eine Verbesserung des Sicherheitsniveaus ausgelegt ist. Zur reinen Analyse der IT-Sicherheit würde schon eine Durchführung der Basis-Sicherheitscheck mit vorheriger Strukturanalyse, Schutzbedarfsfeststellung und IT-Sicherheitskonzeption genügen.

Der Standard bietet verschiedene Möglichkeiten, Kosten und Aufwand zu verringern. Dies ist vor allem für KMUs, die ein geringeres Budget haben, interessant. Es wird darauf hingewiesen, dass oft organisatorische Sicherheitsmaßnahmen teurere technische Lösungen ersetzen können, wobei hier die Einhaltung und damit der Schutz vor dem Risiko schwieriger zu überprüfen ist (vgl. [19], S. 30f). Für kleine Unternehmen ist bereits ein einzelner IT-Sicherheitsbeauftragter für die Sicherheitsorganisation ausreichend, der auch andere Aufgaben im Unternehmen übernehmen kann. Außerdem müssen nicht alle Maßnahmen umgesetzt werden, sie können begründet als „entbehrlich“ gekennzeichnet werden. Dies ist vor allem bei kostenintensiven Maßnahmen, die für eine kleine Infrastruktur nicht benötigt werden, relevant. Eventuell kann auf eine Überwachung der Maßnahmen verzichtet werden, beispielsweise zu Gunsten von monatlichen Statusmeetings, in denen der Fortschritt der Umsetzung anhand konkreter Beispiele überprüft wird. Nach der vollständigen Implementierung schlägt der BSI-Standard 100-2 für kleine Unternehmen einen jährlichen Check der IT-Systeme vor, zusammen mit einer Prüfung der Dokumentationen auf Aktualität und einem Workshop, in der aufgetretene Probleme analysiert werden können (S. 140, [19]).

4.3 Payment Card Industry Data Security Standard

Der Payment Card Industry Data Security Standard (PCI DSS) ist ein vom PCI Security Standards Council veröffentlichter Standard, der für alle Unternehmen, die Kreditkartendaten speichern, verarbeiten oder übermitteln, verpflichtend ist. Das Council ist ein Zusammenschluss der wichtigsten Kreditkartenorganisationen, der für mehr Sicherheit im Zahlungsverkehr sorgen soll.

Dies soll durch zwölf überwiegend technische Anforderungen (siehe Abbildung 4.3.1) erreicht werden, die jeweils in Teilanforderungen untergliedert sind. Des Weiteren ist für die einzelnen Daten auf der Kreditkarte festgelegt, ob eine Speicherung zulässig und eine Verschlüsselung notwendig ist.

Ebene

Der Standard erfordert sowohl organisatorische Maßnahmen (wie beispielsweise Schulungsmaßnahmen und weitere in der Informationssicherheits-Richtlinie festgelegte Verfahren) als auch technische Anweisungen, wobei letztere aufgrund des Einrichtungsaufwands zunächst die größere Hürde für KMUs darstellen. Die Methodik zur Erfüllung der Anforderung wird nicht konkret beschrieben, da der Standard vorrangig zum Ziel hat, die IT-Sicherheit gegen ein vorgegebenes Level zu überprüfen und keine Anleitung zum Erreichen eines Sicherheitsniveaus bietet.

¹⁰ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/gskurs_pdf.pdf, aufgerufen am 11.10.2010.

¹¹ https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html, aufgerufen am 11.10.2010.

¹² <http://v.de/>, aufgerufen am 04.08.2010.

1. Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
2. Ändern der vom Anbieter festgelegten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter
3. Schutz gespeicherter Karteninhaberdaten
4. Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
5. Verwendung und regelmäßige Aktualisierung von Antivirensoftware
6. Entwicklung und Wartung sicherer Systeme und Anwendungen
7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach geschäftlichem Informationsbedarf
8. Zuweisung einer eindeutigen ID für jede Person mit Computerzugriff
9. Beschränkung des physischen Zugriff auf Karteninhaberdaten
10. Verfolgung & Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
11. Regelmäßiges Testen der Sicherheitssysteme und -prozesse
12. Befolgung einer Informationssicherheits-Richtlinie

Abbildung 4.3.1: Die 12 Anforderungen von PCI DSS

Voraussetzungen

Der Standard ist auf die Absicherung von Kreditkartendaten zugeschnitten. Ohne deren Verwendung ist es nicht sinnvoll, eine Zertifizierung zu beantragen. Viele der Anforderungen sind allerdings universell einsetzbar.

Prüfung

Die Zertifizierung erfolgt durch den Anbieter der Kreditkarten-Dienstleistung¹³¹⁴ [31]. Ihm müssen je nach Händler-Level verschiedene Dokumente vorgelegt werden, die von anerkannten Scan-Anbietern¹⁵ (Approved Scanning Vendor - ASV) bzw. qualifizierten Sicherheitsgutachtern¹⁶ (Qualified Security Assessor - QSA) ausgestellt werden.

SBF-Validierungstyp	Beschreibung	SBF
1	Händler, bei denen Karte nicht vorliegt (E-Commerce oder Bestellung per Post/Telefon), alle Karteninhaber-Datenfunktionen extern vergeben	A
2	Nur-Abdruck-Händler ohne Karteninhaber-Datenspeicher	B
3	Händler mit eigenständigen Terminals mit Dial-Out-Funktion, kein Karteninhaber-Datenspeicher	B
4	Händler mit Zahlungsanwendungssystemen, die mit dem Internet verbunden sind, kein Karteninhaber-Datenspeicher	C
5	Alle anderen Händler (nicht in den Beschreibungen für SBF A-C oben enthalten) und alle Dienstleister, die von einer Zahlungsmarke als für das Ausfüllen eines SBF qualifiziert definiert werden	D

Tabelle 4.4: Tabelle zur Auswahl des Selbstbeurteilungsfragebogens aus [30]

¹³ <http://www.mastercard.com/de/merchant/acquirer.html>, aufgerufen am 06.10.2010.

¹⁴ http://www.visa.de/visa_akzeptieren/haendlerbanken/main.jsp, aufgerufen am 06.10.2010.

¹⁵ https://www.pcisecuritystandards.org/pdfs/asv_report.html, aufgerufen am 06.10.2010.

¹⁶ https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf, aufgerufen am 06.10.2010.

Der Zertifizierungsprozess beginnt mit einem Fragebogen, den das Unternehmen ausfüllen muss (Selbstbeurteilungsfragebogen - SBF). Abhängig von der Art der Verwendung und Speicherung der Kreditkartendaten (siehe Tabelle 4.4) werden Fragen zum Unternehmen allgemein und zum technischen Zustand der Infrastruktur gestellt. Für Webshops sind dabei nur zwei SBF-Typen relevant: A, wenn die Verwaltung der Kreditkartendaten ausgelagert ist oder D, wenn Kreditkartendaten gespeichert werden.

Die Unternehmen, die Kreditkartendaten nutzen, werden je nach Anzahl der Transaktionen in verschiedene Level kategorisiert (siehe Tabelle 4.5). Abhängig vom Level werden nun Überprüfungen durchgeführt: Bei einem Security Scan wird vom ASV eine automatische Überprüfung über das Internet durchgeführt. So werden von außen erreichbare Schwachstellen ermittelt, die zur Kompromittierung von Kreditkartendaten führen könnten. Hierbei werden implizit einige der zwölf Anforderungen überprüft. Nach Abschluss des Scans wird ein Scanreport generiert, mit dem das Unternehmen gegebenenfalls Probleme erkennen und beheben kann. Hat der Scan Schwachstellen erkannt, ist ein Rescan nach Behebung der Probleme erforderlich.

Level	Kriterium	Self-Assessment	Security Scan	Security Audit
1	> 6 Mio. Transaktionen pro Jahr oder Gefährdung der Daten	-	4 x pro Jahr	1 x pro Jahr
2	1 Mio. - 6 Mio. Transaktionen pro Jahr	1 x pro Jahr + Extra-Formular	4 x pro Jahr	-
3	20.000 - 1 Mio. Transaktionen pro Jahr	1 x pro Jahr	4 x pro Jahr	-
4	alle anderen	1 x pro Jahr	4 x pro Jahr	-

Tabelle 4.5: Auflagen des PCI-Standards für unterschiedliche Level

Bei Händlern mit vielen Transaktionen oder einem Datendiebstahl in der Vergangenheit wird zusätzlich ein Security Audit vom QSA durchgeführt. Der Audit wird beim zu zertifizierenden Unternehmen durchgeführt und beinhaltet die Überprüfung der Serverräume und Interviews mit Mitarbeitern.

Wurden alle Überprüfungsmaßnahmen bei einem Unternehmen durchgeführt, ohne dass Mängel entdeckt wurden, so ist es PCI-konform. Allerdings müssen die zeitlich festgelegten Folge-Überprüfungen zufriedenstellend verlaufen, um die Zertifizierung zu erhalten.

Aufwand und Kosten

Die Kosten können - abhängig vom Level - sehr unterschiedlich sein. Sie teilen sich auf in einmalige Kosten für die benötigte und eventuell noch nicht vorhandene Infrastruktur wie Firewalls, die Kosten für die Überprüfungsmaßnahmen und Kosten zur Erhaltung der Konformität¹⁷. Dazu kommt noch der Arbeitsaufwand, um die Anforderungen zu erfüllen. Deshalb lagern KMUs die Verwaltung der Kreditkartendaten oft aus, um so Kosten und Aufwand zu sparen.

Bei einem der oben genannten Dienstleister kosten 4 Security Scans beispielsweise 780 Euro¹⁸. Der Standard selbst ist kostenlos erhältlich¹⁹.

Nutzen und Anpassbarkeit

Der Standard ist verpflichtend für Unternehmen, die Kreditkartendaten verarbeiten. Wird er nicht eingehalten, so drohen bei einem Diebstahl von Kreditkartendaten Konsequenzen: Es kann zu hohen Strafzahlungen bis hin zum Ausschluss von der Kreditkartenbezahlung kommen. In jedem Fall werden Händler

¹⁷ http://www.solidcore.com/assets/PCI_Cost_Analysis.pdf, aufgerufen am 10.10.2010.

¹⁸ Preise zzgl. Mehrwertsteuer, http://pci.usd.de/files/public/download/german/usd_PCI_DSS_Vulnerability_Scans_2010_de.pdf, aufgerufen am 17.08.2010.

¹⁹ https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml, aufgerufen am 17.08.2010.

mit Level 2 bis 4 automatisch auf Level 1 hochgestuft, was zu höheren Kosten führt. Abgesehen davon ist ein Datendiebstahl oft mit Ansehens- und Vertrauensverlust beim Kunden verbunden, was zu Umsatzeinbrüchen führen kann. Tritt ein solcher Diebstahl auf, obwohl das Unternehmen PCI-zertifiziert ist, so werden die Strafgebühren gesenkt oder erlassen (Safe-Harbour-Lösung). Die aufgestellten Anforderungen sind sicherheitsorientiert, ihre Umsetzung ist für die Verbesserung der IT-Sicherheit förderlich. Die detaillierten Anforderungen erlauben wenig Interpretationsfreiheit und sind alle verpflichtend. Daher sind kaum Anpassungen möglich.

4.4 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) ist ein Ansatz zur Risikoanalyse bezüglich Informationssicherheit, der auf den drei Komponenten Bedrohungen, Werte und Schwachstellen basiert. Er wurde vom Software Engineering Institute (SEI) der Carnegie Mellon University entwickelt und adressiert sowohl organisatorische als auch technische Risiken.

Der Vorgang der Risikoanalyse ist aufgeteilt in drei Phasen mit jeweils 2-4 Prozessen.

In Phase 1 werden die wichtigsten Werte der Organisation (critical assets) gesammelt sowie Sicherheitsanforderungen und Bedrohungen für jeden Wert beschrieben, sodass am Ende der Phase Bedrohungsprofile vorliegen. Der Prozess soll von allen Hierarchieebenen (Management, technische Mitarbeiter) unterstützt werden, um alle relevanten Werte zu bestimmen.

Phase 2 beschäftigt sich mit der Infrastruktur: Für jeden kritischen Wert werden die zugehörigen Komponenten bestimmt und deren Schutzniveau und Schwachstellen festgestellt.

Für jeden Wert wird in Phase 3 das Risiko ermittelt und festgelegt, wie diesem begegnet werden soll. Resultat dieser Phase ist eine Schutzstrategie für das Unternehmen und Abschwächungspläne für die Risiken der kritischen Werte.

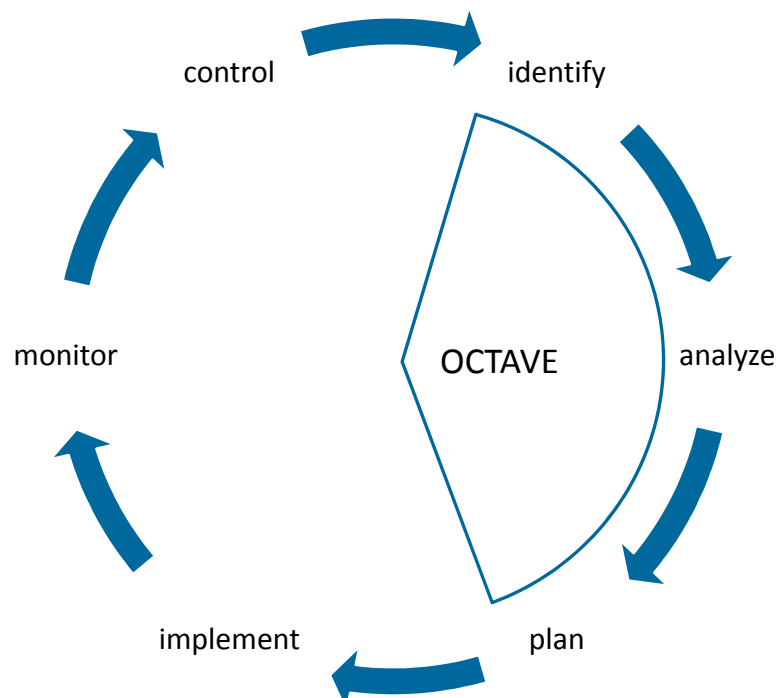


Abbildung 4.4.1: Einordnung von OCTAVE in einen generischen Risikomanagement-Prozess (aus [1])

Mit OCTAVE werden Risiken identifiziert und analysiert sowie eine Schutzstrategie entwickelt. Damit ist es kein kontinuierlicher Prozess, der als PDCA-Zyklus dargestellt werden kann. Das gesamte Risikomanagement kann aber durchaus als ein Kreislauf dargestellt werden, OCTAVE findet dabei zu Beginn einer

Plan-Phase statt (siehe Grafik 4.4.1).

OCTAVE richtet sich generell an größere Unternehmen (in [1] ist ein Richtwert von 300 Mitarbeitern angegeben), für kleinere Unternehmen mit weniger als 100 Mitarbeitern wurde OCTAVE-S entwickelt. Letzteres besitzt weniger Prozesse in den einzelnen Phasen, da zu Beginn ein aufwändiges, formales Sammeln von Daten in allen Managementschichten entfällt und auch die technische Analyse verkürzt wurde, um Mitarbeiterressourcen zu sparen. Daher ist Phase 1 weniger aufwändig und es wird weniger Expertenwissen im Bereich der Schwachstellenanalyse vorausgesetzt. Dies ist zulässig, da kleinere Firmen weniger Hierarchie-Ebenen sowie eine übersichtlichere, oftmals sogar ausgelagerte technische Infrastruktur besitzen. Dennoch ist es möglich, Teile von OCTAVE in OCTAVE-S zu integrieren, um die Risikoanalyse auf die Bedürfnisse des Unternehmens anzupassen.

Ebene

Der Fokus liegt auf den kritischen Werten des Unternehmens, es wird also von der Wertschöpfungskette ausgegangen und daraufhin die relevanten technischen Komponenten analysiert. Die organisatorische Sichtweise kommt in Phase 1 zum Einsatz, die technische in Phase 2. Die in Phase 3 entwickelte Schutzstrategie kann sowohl technische als auch organisatorische Komponenten besitzen.

Voraussetzungen

Um eine Risikoanalyse nach OCTAVE durchführen zu können, wird ein kleines Team - idealerweise von drei bis fünf Mitarbeitern - benötigt, welches sich mit den Unternehmenswerten und der Infrastruktur auskennt.

Prüfung

OCTAVE ist ein reines Vorgehensmodell und bietet keine Zertifizierungsmöglichkeit. Die Anwendung von OCTAVE kann allerdings andere Zertifizierungen, zum Beispiel nach ISO 27001, vereinfachen, da es die dort geforderte Risikoanalyse ausführt.

Aufwand und Kosten

Zur Durchführung von OCTAVE muss ein kleines Team einige Wochen Arbeitszeit aufwenden, OCTAVE-S benötigt in der Regel nur einige Tage ([1], S. 20). Der größte Teil der Kosten entfällt daher auf das Personal. Der Standard selbst ist kostenfrei erhältlich²⁰.

Nutzen und Anpassbarkeit

Durch die Risikoanalyse werden Bedrohungen entdeckt und priorisiert. Dies liefert Rückschlüsse auf das momentane Sicherheitsniveau der Infrastruktur. Des Weiteren werden in der dritten Phase Gegenmaßnahmen entworfen, die anschließend umgesetzt werden können.

Das zuvor bereits erwähnte OCTAVE-S ist eine auf KMUs zugeschnittene Variante von OCTAVE, welche weniger Mitarbeiterressourcen und Spezialwissen, wie es eher in größeren Unternehmen vorhanden ist, benötigt. Bei einer komplexen IT-Infrastruktur besteht die Möglichkeit, dennoch die genaueren Analysemethoden von OCTAVE zu verwenden.

4.5 ITIL

Die Information Technology Infrastructure Library (ITIL) ist eine Sammlung von Best Practices für die Umsetzung des IT-Service-Managements in Unternehmen. Es handelt sich hierbei um keinen reinen IT-Sicherheits-Standard, es sind lediglich sicherheitsrelevante Anteile enthalten. ITIL kann als Basis für eine Zertifizierung von ISO/IEC 20000, einer Norm zum IT-Service-Management, dienen. Der Standard wird vom Office of Government Commerce (OGC) betreut und liegt momentan in der Version 3.0 vor. Er besteht aus einem Kernbereich (ITIL Core), Ergänzungen (ITIL Complementary Guidance) und den ITIL

²⁰ <http://www.cert.org/octave/>, aufgerufen am 29.09.2010.

Web Support Services ([29], S. 9). Im Folgenden werden nur die Kernbereiche vorgestellt, da diese als Überblick über den Standard und zur Betrachtung der Sicherheitsfeatures ausreichen. Mithilfe eines organisierten IT-Service-Managements sollen die Geschäftsprozesse durch die IT unterstützt werden. Dabei werden vor allem solche adressiert, die notwendig sind für den Betrieb der Infrastruktur eines Unternehmens, das auf das Bereitstellen von Services für Kunden ausgerichtet ist (S. 10, [40]).

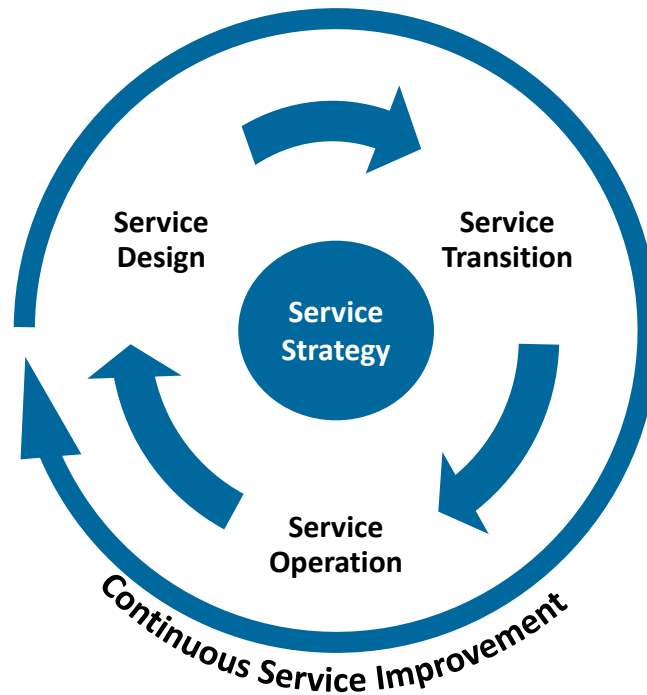


Abbildung 4.5.1: ITIL Service Lifecycle (vereinfacht, aus [38])

Ähnlich wie ISO 27001 ist ITIL prozessorientiert und folgt dem PDCA-Zyklus, der hier als „Service Lifecycle“ bezeichnet wird (siehe Abbildung 4.5.1). Der Standard besteht aus 5 Bereichen: Service Strategy, Service Design, Service Transition, Service Operation und Continuous Service Improvement. Der Bereich *Service Strategy* liefert Best-Practice-Ansätze zur Entwicklung einer Strategie für das Service Management. Dabei steht zunächst die Analyse im Vordergrund: Die Umgebung („market space“) der späteren Services wird definiert; Kunden, Bedarf und Möglichkeiten werden analysiert. Als Rahmenbedingungen bei der Definition von Strategien müssen Kosten, Risiken und das Ziel, die aktuelle Situation zu verbessern, beachtet werden. So wird eine gewinnbringende Strategie gebildet, die einen Nutzen für den Kunden ermöglicht. Für diese werden die benötigten Fähigkeiten und Betriebsmittel („strategic assets“) ermittelt. Abschließend werden die Ergebnisse in Plänen und Richtlinien festgehalten.

Die Analyse von Kundenanforderungen und anschließende Umwandlung in passende Services wird mit dem Bereich *Service Design* vollzogen. Dafür müssen verschiedene Prozesse durchgeführt werden. Es soll ein Service-Katalog, der die Geschäftsprozesse des Kunden auf die benötigten Services und die Services auf die Hardware abbildet, erstellt werden. Die Vereinbarungen mit Kunden sind in längerfristigen Verträgen, sogenannten Service Level Agreements (SLA), festzuhalten. Außerdem muss die Kapazität und Grad der Verfügbarkeit der benötigten Ressourcen analysiert und ein Notfallmanagement implementiert werden. Mit eventuellen Zulieferern/externen Dienstleistern müssen entsprechende Verträge („underpinning contracts“) abgeschlossen werden. Ein Prozess des Bereichs Service Strategy, der Sicherheitsaspekte berücksichtigt, ist das Information Security Management, welches die im Service Level Agreement festgelegten Sicherheitsanforderungen aufrechterhalten soll. Dies soll durch Implementierung von Sicherheitsfunktionen ermöglicht werden. Des Weiteren müssen aber auch Reaktionen auf Sicherheitsverletzungen (z.B. in Form von Notfallplänen) definiert werden.

Der Bereich *Service Transition* umfasst die Entwicklung und Übergabe von neuen und die Änderung und Verbesserung von bereits implementierten Services. Dazu werden Kernprozesse wie Change Management benötigt, welches Änderungen verwaltet, indem sie ordnungsgemäß geplant, dokumentiert und gegebenenfalls nach Auswirkung und Dringlichkeit priorisiert werden.

Eine Verwaltung der Configuration Items (CI), also aller Komponenten und Dokumente, hilft, Änderungen nachzuvollziehen. Des Weiteren sollten alle Änderungen getestet und validiert werden, sodass sie die im Service Level Agreement definierten Qualitätskriterien erfüllen. Abschließend ist eine Evaluierung des Prozesses hilfreich, um eventuelle Fehler aufzudecken.

Im Bereich *Service Operation* finden sich Best Practices zum Betrieb und Support der entwickelten Services. Unter anderem werden Verfahren zur Behandlung von Ereignissen, Störungen, Problemen und Service-Anfragen beschrieben. Ein zentrales Modell ist dabei der Service Desk, der alle Anfragen an einem Punkt bündelt und so beispielsweise die Regelungen der Zuständigkeiten vereinfacht.

Als letztes ist es wichtig, eine ständige Verbesserung der Services anzustreben. Im Kapitel *Continual Service Improvement* wird vorgeschlagen, Messungen durchzuführen. Dazu muss zunächst definiert werden, was und wie gemessen wird, beispielsweise durch Implementierung eines Kennzahlensystems. Die Daten werden analysiert, verarbeitet (zum Beispiel in Aktionsplänen) und Korrekturmaßnahmen werden umgesetzt. Dieser Prozess kann nun zyklisch fortgeführt werden, die umgesetzten Korrekturmaßnahmen werden also wiederum überprüft und eventuell weiter angepasst.

Ebene

ITIL beschreibt die Umsetzung des Service Managements mit Hilfe der IT. Dazu gehören organisatorische und auf einem hohen Abstraktionsniveau auch technische Vorgaben, die Sicherheit der IT wird aber nur sehr knapp behandelt.

Voraussetzungen

Um ITIL anwenden zu können, muss das Unternehmen IT-Dienstleistungen für Kunden bereitstellen. Ein Beispiel für solche Unternehmen sind Outsourcing-Dienstleister. Webshops gehören eher nicht dazu, da sie den Kunden lediglich Produkte - in der Regel ohne weiteren Service - verkaufen. Aufgrund der vielen Prozesse der verschiedenen Bereiche ist der Standard eher für größere Unternehmen geeignet.

Prüfung

Eine Zertifizierung eines Unternehmens nach ITIL ist nicht möglich. Sie kann aber nach ISO/IEC 20000 erfolgen, da diese Norm sich auf das Service Management in der IT konzentriert und auf die Prozessbeschreibungen von ITIL ausgerichtet ist. Die ITIL-Zertifikate und -Trainings²¹ überprüfen das ITIL-Fachwissen einzelner Mitarbeiter/Manager.

Aufwand und Kosten

Wenn keine Zertifizierung nach ISO 20000 angestrebt wird, besteht die Möglichkeit, auch nur einige, ausgewählte Best Practices umzusetzen. Ohne Zertifizierung sind die Kosten nur vom Arbeitsaufwand abhängig, der für die Umsetzung erforderlich ist. Der Standard selbst ist kostenpflichtig.

Nutzen und Anpassbarkeit

Der Nutzen für Webshops ist in Bezug auf Absicherung der Infrastruktur begrenzt: Es wird zwar auf Sicherheitsaspekte bei der Entwicklung von Services eingegangen, dabei wird sich jedoch vor allem auf die mit dem Kunden im Service Level Agreement (SLA) vereinbarten Anforderungen bezogen. ITIL ist nicht auf Sicherheit fokussiert und überhaupt nur schwer auf Webshops anwendbar: Ein Webshop hat zwar Kunden, mit ihnen wird aber kein SLA abgeschlossen. Die erbrachte Dienstleistung beinhaltet lediglich die Lieferung der bestellten Ware, was nicht als längerfristiger Service-Vertrag angesehen werden kann. Die Anpassbarkeit ist durch die Vereinbarungen des SLAs gegeben.

²¹ <http://www.ital.org/de/zumkoennen/ital/ital/zertifizierungsmodell.php>, aufgerufen am 06.10.2010.

4.6 Cobit

Cobit (Control Objectives for Information and Related Technology) ist ein von der ISACA (Information Systems Audit and Control Association) entwickelter prozessorientierter IT-Governance-Standard²², der IT-Sicherheit nur nebensächlich thematisiert. Er bietet ein Framework zu Aufbau und Analyse eines IT-Systems zur Unterstützung der Unternehmensziele. Aktuell liegt Cobit in der Version 4.1 vor, an der sich auch dieser Abschnitt orientiert.

Ziel des Standards ist die effiziente Unterstützung der Geschäftsprozesse des Unternehmens durch die IT. Andere, spezifischere Standards wie ITIL für Service Management oder das Capability Maturity Model Integration <http://www.sei.cmu.edu/cmmi/>, aufgerufen am 06.10.2010 zur Qualitätsbewertung können integriert und so parallel verwendet werden. Die Abbildung 4.6.1 liefert einen Überblick über die Struktur von Cobit.

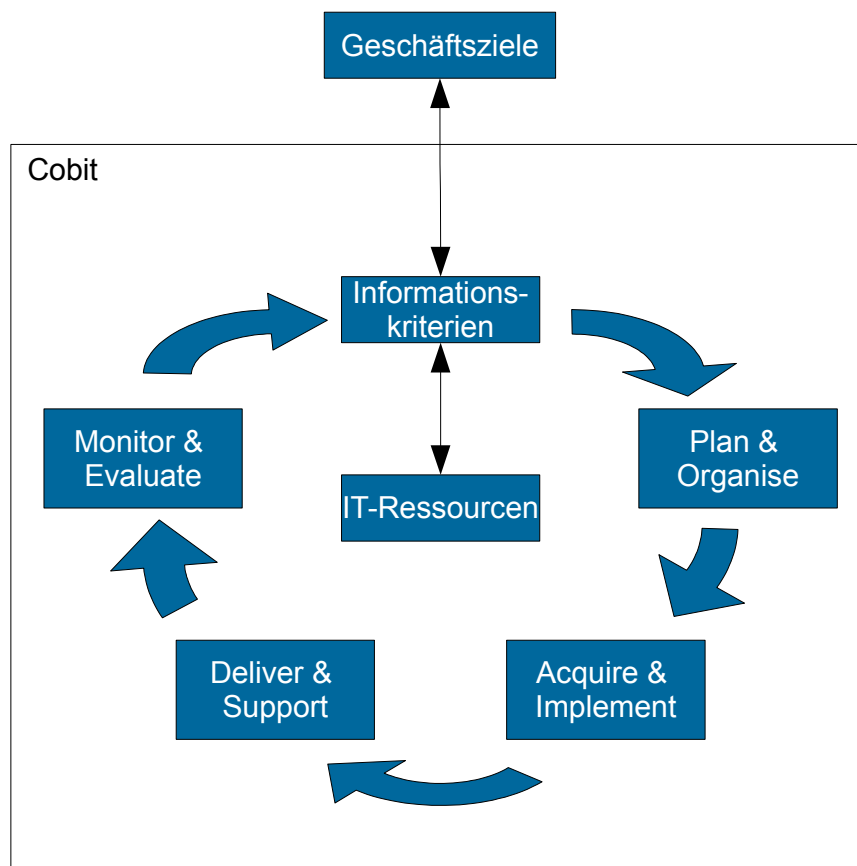


Abbildung 4.6.1: Überblick über das Cobit-Framework, entnommen aus [20]

Ein wichtiger Teil des Frameworks ist das Management der durch die IT verarbeiteten Informationen. Cobit besitzt sieben Informationskriterien (vergleichbar mit den Schutzzielen): Neben den Sicherheitseigenschaften Vertraulichkeit, Verfügbarkeit und Integrität zählen Effektivität, Effizienz, Verlässlichkeit und die Einhaltung der gesetzlichen Richtlinien dazu.

Die IT wird bei Cobit in vier Klassen aufgeteilt:

- **Anwendungen** beinhalten alle automatischen und manuellen Verfahren der Informationsverarbeitung

²² IT-Governance beschreibt die Führung und Kontrolle der IT durch die Unternehmensführung, um eine bestmögliche Unterstützung der Geschäftsprozesse zu erreichen.

-
- **Informationen** sind Daten des Unternehmens in jeglicher Form
 - **Infrastruktur** beschreibt Einrichtungen und Technologie
 - **Personal** sind Mitarbeiter, die die Informationssysteme betreuen

Mithilfe der Ressourcen wird durch ein Prozessmodell versucht, die Informationskriterien zu etablieren. Cobit enthält 34 Prozesse, diese sind aufgeteilt in vier Domänen:

- Plan & Organise (PO) beinhaltet die Ausarbeitung der IT-Strategie zur Umsetzung der Geschäftsziele. Unter anderem werden mögliche Risiken analysiert und Prozesse definiert sowie die Mitarbeiter bereitgestellt.
- Acquire & Implement (AI) hat zum Ziel, die IT-Strategie umzusetzen. Dazu werden beispielsweise Machbarkeitsstudien durchgeführt und Anwendungen und Infrastruktur beschafft und installiert.
- Deliver & Support (DS) enthält Prozesse, die die Auslieferung und Wartung der benötigten Services unterstützen. Dazu gehört das Festlegen von Service Levels, Sicherstellen der Verfügbarkeit und Sicherheit, die Schulung von Benutzern und ein angemessenes Problem-Management.
- Monitor & Evaluate (ME) befasst sich mit dem Messen der Leistung und der Auswertung der installierten Kontrollmechanismen. Es wird überprüft, ob die vorher vereinbarten Vorgaben eingehalten wurden.

Jeder der 34 Prozesse ist nochmals in kleinere Ziele (sogenannte detaillierte Control Objectives) und Aktivitäten aufgeteilt und durch Ein- und Ausgaben beschrieben. Durch Metriken, die im Prozess selbst definiert sind und ein Reifegradmodell, das den Prozess auf einer Skala von 0-5 bewertet, kann die Qualität der Umsetzung jedes Prozesses ermittelt werden.

Um Aussagen über die Unterstützung der Geschäftsprozesse durch die IT machen zu können, muss die Umsetzung der Prozesse analysiert werden. Deshalb ist das Messen der Performance ein wichtiger Bestandteil von Cobit und wird auf drei Ebenen durchgeführt ([20], S. 20). Mit Hilfe von Metriken innerhalb eines Prozesses, auf Prozessebene und schließlich durch Messungen der ganzen IT und Abgleich mit den Anforderungen des Unternehmens ist eine genaue Analyse des Zustands der IT möglich. Die Metriken sind unterteilt in Kennzahlen, die erst nach einer Zielerreichung zur Verfügung stehen und Indikatoren, die eine momentane Leistung messen.

Der Prozess „Ensure systems security“ (DS5) aus der Domäne „Deliver & Support“ dient im Weiteren als Beispiel für den Aufbau eines Prozesses. Er ist relevant für die Aufgabe, die IT-Sicherheit von Webshops zu evaluieren und zu verbessern und sollte daher einen möglichst hohen Reifegrad erreichen, also gut umgesetzt sein. Die Beschreibung des Prozesses (vgl. [21], S. 117-120) beginnt mit einer allgemeinen Zusammenfassung und stellt dann den Bezug zu den Informationskriterien her. Bei DS5 sind Vertraulichkeit und Integrität primäre Ziele, Verfügbarkeit, Verlässlichkeit und die Einhaltung gesetzlicher Richtlinien sekundäre Ziele.

In elf Kontrollzielen werden die Ziele näher beschrieben. Sie enthalten Anweisungen, das Management der IT-Sicherheit auf der obersten Organisationsebene zu etablieren (DS5.1) sowie einen umfassenden IT-Sicherheitsplan zu entwerfen und zu kommunizieren (DS5.2). Ein Fokus liegt auf der Verwaltung der Benutzer, sie müssen zusammen mit den von ihnen durchgeführten Aktivitäten eindeutig identifizierbar sein (DS5.3) und einem Zugriffsberechtigungssystem unterliegen (DS5.4). Die Sicherheit und Maßnahmen sollten überwacht und überprüft werden (DS5.5) sowie Sicherheitsvorfälle identifiziert und Gegenmaßnahmen festgelegt werden (DS5.6). Sowohl Hardware (DS5.7) als auch Software sollte abgesichert werden, letztere beispielsweise durch Software-Updates und Antivirenprogramme (DS5.9). Die Netzwerksicherheit (DS5.10) und der sichere Austausch sensibler Daten (DS5.11) muss etabliert werden.

Die zur Verschlüsselung eingesetzten kryptographischen Schlüssel müssen verwaltet werden (DS5.8). Des Weiteren sind für den Prozess Ein- und Ausgaben sowie die Aktivitäten und deren Zuständigkeit definiert (vgl. [21], S. 119). Darauf folgen Ziele und Metriken auf den oben angesprochenen drei Ebenen, ein Aktivitätsziel ist beispielsweise das Management der Benutzer und deren Zugriffsbeschränkungen. Entsprechende Metriken des Prozesses DS5 sind sowohl die Anzahl der alten, nicht mehr verwendeten Benutzerkonten als auch die Anzahl der veränderten Zugriffsberechtigungen.

Als nächstes folgt die Beschreibung der Reifegrade. Für einen Reifegrad von 3 („Defined“) müssen IT-Sicherheitsverfahren und Verantwortlichkeiten definiert sein sowie Sicherheitstests durchgeführt und Schulungen angeboten werden. Mithilfe von Risikoanalysen wird eine Planung erstellt und allgemein wird das Sicherheitsbewusstsein durch das Management gefördert.

Ebene

Cobit ist ein Standard für die Schnittstelle zwischen den Geschäftsprozessen und der IT. Es wird top-down, also ausgehend von den Geschäftszielen, eine IT-Strategie aufgebaut und umgesetzt. Sie enthält Anforderungen auf verschiedenen Ebenen, also auch auf der technischen Ebene (wie zum Beispiel im Prozess DS5). Eine Verknüpfung mit anderen Standards ist möglich. Da der Standard nicht auf IT-Sicherheit fokussiert ist, kann es sinnvoll sein, ihn mit technischen Standards dieses Bereiches wie ISO 27001 zu verbinden, beispielsweise wenn weitere Sicherheitsanforderungen an die IT gestellt werden, die über die im Prozess DS5 behandelten Punkte hinausgehen.

Voraussetzungen

Für die Umsetzung des relativ aufwändigen Standards gibt es keine bestimmten Voraussetzungen, es müssen nur ein entsprechendes Wissen und die benötigten Ressourcen vorhanden sein.

Prüfung

Eine Zertifizierung nach Cobit ist nicht möglich.

Aufwand und Kosten

Durch den ganzheitlichen Ansatz dieses Standards wirkt der Aufwand zunächst sehr hoch. Jedoch sind in kleineren Unternehmen manche von Cobit beschriebenen Prozesse nicht notwendig (beispielsweise der Prozess „Manage Third-party Services“ (DS2), wenn keine Leistungen von externen Dienstleistern benötigt werden). Die Auswahl der Prozesse erfolgt über die Geschäftsziele der Organisation oder die Informationsanforderungen aus den Geschäftsprozessen (S.23, [13]). Da für nicht implementierte Prozesse auch keine Kennzahlen erfasst und ausgewertet müssen, verringert sich der Aufwand. Da keine Zertifizierung möglich ist, entstehen nur durch die Umsetzung der Maßnahmen Kosten für das Unternehmen. Der Standard ist kostenfrei erhältlich²³.

Nutzen und Anpassbarkeit

Durch die vielfältigen Kontrollen kann der Status der IT gut überwacht werden. Der Aufwand für die Einrichtung der Prozesse und Metriken kann sehr hoch sein, von Vorteil ist jedoch die dauerhafte Überprüfung. Insbesondere der Prozess „Ensure Systems Security“ (DS5) ist für die Evaluierung und Verbesserung der IT-Sicherheit nützlich.

Einzelne Informationskriterien können unberücksichtigt bleiben, um damit den Aufwand zu reduzieren (S. 17, [22]).

4.7 IDW PS 330

Der vom Institut der Wirtschaftsprüfer (IDW) herausgegebene Standard „IDW Prüfungsstandard: Abschlußprüfung bei Einsatz von Informationstechnologie (IDW PS 33)“ wurde entwickelt, um IT-Systeme

²³ <http://www.isaca.org/KNOWLEDGE-CENTER/COBIT/Pages/Downloads.aspx>, aufgerufen am 11.10.2010.

in die Prüfung von Jahres-, Konzern- und Zwischenabschlüssen einzubeziehen. Die Prüfung beschränkt sich dabei auf den Teil der IT, der Daten verarbeitet oder speichert, die für die Rechnungslegung wichtig sein können. Durch die Anwendung des Standards soll das Risiko von Fehlern im IT-System beurteilt werden können.

Geprüft werden dabei die Ebenen IT-Infrastruktur, IT-Anwendungen, IT-gestützte Geschäftsprozesse, das IT-Umfeld und die IT-Organisation. Zu jeder Kategorie werden Risiken identifiziert, die dann in der Kombination mit anderen Risiken zu IT-Fehlerrisiken führen, sodass die Gefahr von wesentlichen Fehlern in der Rechnungslegung besteht. Beispielsweise sind fehlerhafte Funktionen in Anwendungen, unvollständige Verfahrensregelungen und fehlende Eingabekontrollen von Daten Anwendungsrisiken, die analysiert werden müssen.

Im Standard werden Risikoindikatoren vorgestellt, die Anhaltspunkte für mögliche Risiken bieten und überprüft werden sollen: So muss die Abhängigkeit des Unternehmens zur IT betrachtet werden, besonders wenn wichtige Daten nur in IT-Systemen gespeichert werden. Außerdem weisen größere Änderungen an IT-Systemen oft ein Fehlerpotential auf. Beachtet werden muss außerdem der Kenntnisstand bzw. Ausbildungsgrad der Mitarbeiter und die Umsetzung der Geschäftsstrategie in eine IT-Strategie. Für alle Risiken muss überprüft werden, ob ein IT-Kontrollsystem eingesetzt wird, das auf das Risiko reagiert, indem es verhindert, dass es zu Fehlern in der Rechnungslegung kommen kann (S. 9, [17]).

Ebene

Es werden sowohl technische Vorkehrungen als auch organisatorische Maßnahmen überprüft, im Fokus steht immer die Prüfung der rechnungsrelevanten Systeme.

Voraussetzungen

Der Standard wird im Rahmen von Jahresabschlussprüfungen auf rechnungsrelevante Systeme angewendet. Um einen realistischen Eindruck über das System zu erhalten, sollten zumindest die kritischsten Komponenten überprüft werden.

Prüfung

Die Zertifizierung erfolgt durch einen Wirtschaftsprüfer. Die Prüfung des IT-Systems beginnt mit der Aufnahme des IT-Systems, dazu werden zunächst Informationen über die Ebenen gesammelt.

Die Aufbauprüfung soll die Angemessenheit der Maßnahmen beurteilen, die zur Gewährleistung des IT-Betriebs, der Funktionalität der IT-Anwendungen und der Sicherheit des Systems umgesetzt wurden. Die Eignung der Maßnahme muss dabei sowohl in technischer als auch in personeller und organisatorischer Hinsicht kontrolliert werden. Die Kontrolle findet unabhängig vom Zustand des Systems statt und prüft, ob das System angemessen ist, um den zuvor beschriebenen Risiken zu begegnen. Dies geschieht meist durch Überprüfen von Unterlagen und Arbeitsabläufen oder Befragungen der Mitarbeiter.

Die Funktionsprüfung dient dazu, die Wirksamkeit der umgesetzten Maßnahmen zu beurteilen. Eine Methode ist beispielsweise das Vergleichen von Arbeitsweisen des Unternehmens mit branchenbezogenen Best Practices. Hierfür können interne Dokumentationen und Protokolle des Unternehmens verwendet werden.

Aufwand und Kosten

Der Aufwand ist verhältnismäßig gering, da es sich um einen externen Sicherheitsaudit handelt: Die Prüfung des Systems wird nicht von Mitarbeiter des Unternehmens, sondern von einem Wirtschaftsprüfer durchgeführt. Die Kosten sind abhängig vom Wirtschaftsprüfer, der die Prüfung durchführt.

Nutzen und Anpassbarkeit

Für den IT-Sicherheitsaspekt ist vor allem die Prüfung der IT-Organisation und der IT-Infrastruktur interessant: Letztere beinhaltet einen Check der Maßnahmen zum physischen Schutz und Zugriffskontrollen, die Prüfung der IT-Organisation analysiert die Einhaltung von Sicherheitsrichtlinien wie beispielsweise

die Vorgabe einer Mindestlänge für Passwörter.

Insgesamt ist der Standard aber weniger auf die Absicherung durch Angriffe auf ein System als auf die Erhaltung der rechnungsrelevanten Daten ausgelegt. Deshalb sind Archivierungsverfahren, physischer Schutz und Zugriffskontrolle wichtige Komponenten des Standards, während beispielsweise Antivirenprogramme gar keine Erwähnung finden.

Für KMUs ist interessant, dass die Prüfung bei geringer Komplexität des Prüfgegenstands auf einzelne Funktionen beschränkt werden kann.

4.8 Common Criteria

Die Common Criteria for Information Technology Security Evaluation (CC) beschreiben international standardisierte Kriterien zur Bewertung und Zertifizierung der Sicherheit von Computersystemen bezüglich Funktionalität und Vertrauenswürdigkeit. Sie ersetzen die älteren Information Technology Security Evaluation Criteria (ITSEC), die von der Europäischen Kommission veröffentlicht wurden.

Der Standard umfasst drei Teile, wobei der erste Teil einen Überblick über die Methode gibt und wichtige Grundbegriffe erklärt. Der zweite Teil beschäftigt sich mit den funktionalen Sicherheitsanforderungen und der Dritte mit den Sicherheitsanforderungen bezüglich Vertraulichkeit.

Bei der Evaluierung eines Computersystems nach CC kann zunächst ein Schutzprofil (Protection Profile) erstellt oder ausgewählt werden, welches implementierungsunabhängige Sicherheitsanforderungen an eine Kategorie von Produkten (zum Beispiel Firewalls) enthält. Für das zu evaluierende Produkt, auch Evaluierungsgegenstand (target of evaluation) genannt, müssen dann spezifische Sicherheitsvorgaben (security targets) definiert werden, die die Anforderungen der Schutzprofile konkretisieren. Die Vertrauenswürdigkeit der Evaluation wird in sogenannten „Evaluation Assurance Levels“ (EAL) gemessen, wobei 1 das niedrigste und 7 das höchste EAL ist. Für jedes Level ist eine Menge von Vertrauenswürdigkeits-Anforderungen definiert, die erfüllt sein müssen. Tabelle 4.6 zeigt eine Übersicht über die EAL.

Level	Beschreibung
EAL1	functionally tested
EAL2	structurally tested
EAL3	methodically tested and checked
EAL4	methodically designed, tested, and reviewed
EAL5	semiformally design and tested
EAL6	semiformally verified design and tested
EAL7	formally verified design and tested

Tabelle 4.6: Evaluation Assurance Levels

Die Sicherheitsanforderungen aus Teil 2 und 3 besitzen dieselbe Struktur: Es findet eine Aufteilung in Klassen (siehe Tabelle 4.7) statt, wobei jede Klasse aus verschiedenen Familien besteht, die ihrerseits verschiedene Anforderungs-Komponenten enthält. Abhängigkeiten und Hierarchien zwischen Anforderungskomponenten sind kenntlich gemacht.

Art der Anforderung	zugehörige Klassen
Security Functional Requirements	Security Audit (FAU) Communication (FCO) Cryptographic support (FCS) user data protection (FDP) identification and authentication (FIA) security management (FMT) privacy (FPR) protection of the TSF (FPT) resource utilisation (FRU) TOE access (FTA) trusted path/channels (FTP)
Security Assurance Requirements	protection profile evaluation (APE) security target evaluation (ASE) development (ADV) guidance documents (AGD) life-cycle support (ALC) tests (ATE) vulnerability assessment (AVA) composition (ACO)

Tabelle 4.7: Klassen der Sicherheitsanforderungen

Ebene

Die Common Criteria richten sich ausschließlich an technische Systeme.

Voraussetzungen

Zur Evaluierung des technischen Systems muss eine genaue Spezifikation vorliegen.

Prüfung

Die Evaluation wird von einer vom Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditierten Prüfstelle²⁴ durchgeführt. Die Zertifizierung erfolgt durch das BSI.

Aufwand und Kosten

Der Aufwand ist vor allem von der Komplexität des Evaluationsgegenstandes und des zu erreichenden EAL abhängig. Auch die Wahl des Schutzprofils beeinflusst die Tiefe und den Aufwand der Evaluation. Durch das gründliche Prüfverfahren ist eine Zertifizierung in der Regel sehr teuer.

Nutzen und Anpassbarkeit

Da mit den CC nur eine Evaluierung von technischen Systemen möglich ist, können organisatorische Maßnahmen zum Schutz der Infrastruktur nicht berücksichtigt werden. Aufgrund der Komplexität ist es aufwändig, alle Komponenten des Webshops zu evaluieren. Eine Möglichkeit wäre, sich auf die kritischsten Elemente zu konzentrieren, beispielsweise die Software des Webshops, die auf Webserver läuft. Generell werden die Common Criteria eher von Herstellern von Produkten genutzt, beispielsweise wäre eine CC-Evaluierung bei einer Eigenentwicklung der Shop-Software möglich. Beim Kauf von Shop-Software kann Software bevorzugt werden, die durch CC evaluiert wurde. Durch die Wahl des EAL sind die CC recht anpassbar, ein zu niedriges EAL bringt jedoch keinen großen Nutzen.

²⁴ https://www.bsi.bund.de/cln_174/ContentBSI/Themen/ZertifizierungundAnerkennung/Komformitaetsbestaetigung/Stellen/CC-Liste/cc-itsec-pruefstellen.html, aufgerufen am 06.10.2010.

5 Gütesiegel

Neben Gütesiegeln wie dem „energy star“, der Stiftung Warentest oder Bio-Gütesiegeln, die für Produkte vergeben werden, um deren Qualität oder eine bestimmte Eigenschaft zu garantieren, existieren auch Gütesiegel für Webshops und Datenschutzgütesiegel, auf die hier näher eingegangen werden soll. Durch die immer größere Anzahl an Shops sind sie für Konsumenten zu einem wichtigen Anhaltspunkt bei der Kaufentscheidung geworden¹. Fast die Hälfte der Befragten einer Studie der Europäischen Union[12], die Gütesiegel kannten, gaben an, dass die Präsenz eines Gütesiegels einen Webshops vertrauenswürdiger macht. Die Siegel bieten nicht nur Orientierung für Kunden, sondern werden von zertifizierten Webshops auch als Marketing-Werkzeug verwendet.

Die meisten Gütesiegel versuchen, möglichst viele verschiedene Kriterien abzudecken. Es wird beispielsweise neben der Datensicherheit die Benutzbarkeit des Shops evaluiert. Die Initiative D21 hat Kriterien für Gütesiegel aufgestellt, die im Folgenden analysiert werden. Diese Kriterien werden von vier Gütesiegeln erfüllt, die mit ihren eigenen Anforderungskatalogen beschrieben werden. Anschließend folgen zum Vergleich zwei nicht von D21 empfohlene Gütesiegel für Webshops und schließlich mehrere auf Datenschutz spezialisierte Gütesiegel.

Die Analyse des Nutzens basiert bei den Gütesiegeln auf den Anforderungen der Qualitätskriterien, die oft allgemein gehalten sind. Die Evaluationsmethoden der Gütesiegel-Anbieter sind nicht öffentlich.

5.1 Initiative D21

Die Initiative D21² ist ein gemeinnütziger Verein, der aus Vertretern von Politik und Wirtschaft besteht und es sich zum Ziel gesetzt hat, die Entwicklung der digitalen Gesellschaft durch verschiedene Projekte zu fördern.

Dazu gehören auch die Empfehlungen für Online-Gütesiegel³, die ein Referenzmodell für Anbieter, Online-Händler und Verbraucher darstellen (S. 2, [7]). Von D12 empfohlene Gütesiegel werden durch ein aus Experten bestehendes Monitoring Board der Initiative überwacht. Dabei werden die Qualitätskriterien in halbjährigen Treffen gemeinsam weiterentwickelt und ihre Einhaltung geprüft.

Die Qualitätskriterien [7] sind unterteilt in thematisch abgegrenzte Bereiche, die jeweils aus mehreren Anforderungen bestehen können. Beispielsweise werden Auflagen an den Bestellvorgang, die Vertragsbedingungen und den Datenschutz gestellt. Für die Evaluation der IT-Sicherheit ist vor allem der Unterpunkt „Datensicherheit“ relevant. Hier wird gefordert, dass sowohl die Daten des Anbieters (dazu gehören sämtliche Informationen zu den angebotenen Waren) als auch alle Daten, die zur Geschäftsabwicklung notwendig sind, durch ein IT-Sicherheitskonzept geschützt werden. Schutzziele sind hierbei Integrität und Authentizität der Daten des Anbieters und Integrität und Vertraulichkeit der Daten zur Geschäftsabwicklung. Das Sicherheitskonzept muss Maßnahmen aufweisen, die „allen relevanten Bedrohungen in angemessener Weise entgegenwirken“ (S. 12, [7]).

Geschützt werden muss sowohl die Infrastruktur und die Software als auch die Datenübertragung mit dem Kunden, zum Beispiel durch den Einsatz von Verschlüsselung oder elektronischen Signaturen. Der Zugriff auf personenbezogene Daten muss mit Identifizierungs- und Authentifizierungsverfahren beschränkt werden, um unberechtigte Einsicht oder Manipulation zu verhindern.

Die weiteren Anforderungen sind größtenteils kundenorientiert formuliert. Beispielsweise ist geregelt,

¹ eResult-Studie „Relevanz von Gütesiegeln“:

http://www.eresult.de/studien_artikel/forschungsbeitraege/guetesiegel.html, aufgerufen am 19.09.2010.

² <http://www.initiatived21.de>, aufgerufen am 11.10.2010.

³ <http://www.internet-guetesiegel.de>, aufgerufen am 11.10.2010.

dass der Kunde über eingesetzte Cookies informiert werden muss und er über technische Anforderungen, wie bestimmte Software, die für die sichere Benutzung des Webshops benötigt wird, Informationen erhält. Auch über mögliche Risiken, die durch das Herunterladen von Programmen entstehen, sollte der Kunde informiert werden.

Außerdem müssen die durch D21 empfohlenen Anbieter ihre eigenen Qualitätskriterien auf ihrer Webseite veröffentlichen und es Verbrauchern ermöglichen, Beschwerden gegen zertifizierte Shops einzulegen. Momentan sind die Gütesiegel Trusted Shops, s@fer shopping, internet privacy standards und EHI Geprüfter Online-Shop von D21 empfohlen.

5.1.1 Trusted Shops

Die Trusted Shops GmbH ist mit 8363⁴ nach dem gleichnamigen Gütesiegel zertifizierten Shops der größte Gütesiegel-Anbieter für Webshops. Neben dem Gütesiegel werden verschiedene Audits angeboten, unter anderem ein Security-Audit, der sich speziell auf technische Schwachstellen konzentriert. Dieser wird in Kapitel 6.3 näher erläutert.

Für die Zertifizierung müssen Qualitätskriterien⁵ erfüllt werden, die unterschiedliche Bereiche des Webshops abdecken und beispielsweise Anforderungen an den Liefer- und Bestellprozess sowie an die Allgemeinen Geschäftsbedingungen enthalten.

Ein Unterpunkt des Kapitels „Datenschutz und Datensicherheit“ fordert ein geeignetes IT-Sicherheitskonzept, um Kundendaten zu schützen und Missbrauch zu vermeiden. Dazu gehört das Einsetzen von Verschlüsselungsverfahren, eine Zugriffs- und Zutrittskontrolle und das Einsetzen „sicherer Server“. Überprüft werden auch die e-mails mit Login-Daten, die dem Kunden gesendet werden, sowie die Manipulierbarkeit von URLs, die zu Kundendaten führen. Zahlungsinformationen müssen verschlüsselt übertragen werden. Insgesamt orientieren sich die Anforderungen sehr stark an den Vorgaben von D21.

Ebene

Die Qualitätskriterien enthalten vor allem organisatorische und technische Anforderungen, sowohl an die Webseite selbst als auch an die verkauften Waren und die Bestell- und Lieferprozesse. In einem Audit wird die Konformität zum Kriterienkatalog mit Hilfe von Checklisten überprüft.

Bedingungen

Die Zertifizierung können nur Webshops erwerben, da sie speziell auf sie zugeschnitten ist.

Prüfung

Es werden mehr als 100 Kriterien geprüft. Wenn bei einer Prüfung Mängel festgestellt wurden, sind diese im Prüfungsprotokoll vermerkt. Es sind dabei nicht nur die unerfüllten Anforderungen beschrieben, sondern es werden auch Beispiele gegeben, wie sie erfüllt werden können. Nun hat das Unternehmen die Möglichkeit, die genannten Punkte zu verbessern, sodass nach einer weiteren Prüfung, bei der alle Qualitätskriterien erfüllt sind, das Zertifikat ausgestellt werden kann.

Die Prüfung wird ausschließlich über das Internet vorgenommen, beispielsweise durch Inspektion der Webseite und Durchführung von typischen Benutzer-Aktionen.

Getestet werden beispielsweise die SSL-Verschlüsselung, die Übertragung der Login- und Kontodaten und die Manipulierbarkeit der URLs von kundenspezifischen Seiten. Nach dieser Erstprüfung, in der die Konformität zu den Anforderungen festgestellt wird, folgen jährliche Prüfungen. Sofern diese ergeben, dass der Webshop die Qualitätskriterien einhält bzw. die aufgetretenen Mängel vor einer Nachprüfung beseitigt werden, bleibt das Gütesiegel erhalten.

⁴ <http://www.trustedshops.de/profil/>, aufgerufen am 18.10.2010.

⁵ http://www.trustedshops.de/shopbetreiber/pdf_download/TS-QAL.pdf, aufgerufen am 11.10.2010.

Aufwand und Kosten

Für den Erwerb des Gütesiegels fallen monatliche Kosten an, die sich je nach Umsatz des Shops und Funktionsumfang der Mitgliedschaft berechnen, mindestens jedoch 59 € im Monat. Beim Einsatz von vorzertifizierter Software⁶ sinkt die monatliche Gebühr um 10 €.

Nutzen und Anpassbarkeit

Durch eine Zertifizierung ist die Erfüllung der in den Qualitätskriterien enthaltenen Sicherheitsanforderungen gewährleistet, die sehr kurz gefasst sind.

Der vorgegebene Katalog an Kriterien lässt keine Anpassung zu, dies ist allerdings auch nicht notwendig, da das Gütesiegel schon auf Webshops zugeschnitten ist.

5.1.2 S@fer Shopping

Der TÜV Süd hat zwei Gütesiegel etabliert, die Verbraucher auf vertrauenswürdige Internet-Angebote hinweisen sollen. Für Webseiten ohne Einkaufsvorgänge wird das Zertifikat „s@fer website“ angeboten, für alle anderen „s@fer shopping“, wobei es zusätzlich noch Anforderungskataloge für Versicherungen und Händler der Reisebranche gibt. Im Folgenden liegt der Fokus auf dem „s@fer shopping“-Gütesiegel, welches mit 137 Zertifikaten eine größere Rolle spielt als „s@fer website“ mit 11 Zertifikaten und außerdem für Webshops besser geeignet ist.

Die Anforderungen des Gütesiegels sind in vier Kapitel unterteilt: Organisatorische Anforderungen, Datensicherheit, Datenschutz und Online-Inhalte und Prozesse.

Die organisatorischen Anforderungen beinhalten unter anderem die Anweisung, dass die Konformität zu den Anforderungen und deren Einhaltung bewertet und sichergestellt und eine ständige Verbesserung angestrebt werden soll. Das nächste Kapitel, Datensicherheit, ist am wichtigsten für die IT-Sicherheit der Webshops. Die hier aufgeführten Auflagen gleichen den grundsätzlichen Anforderungen der Initiative D21: Es muss ein geeignetes Sicherheitskonzept verwaltet werden, welches Maßnahmen definiert, die „allen relevanten Bedrohungen in angemessener Weise entgegen“ wirken⁷. Auch die Einrichtungen, Prozesse und der Datenübertragungsweg müssen gesichert und Zugriffsrechte für Dateien vergeben werden. Teilweise gehen die Auflagen aber auch über die D21-Anforderungen hinaus: So muss schon bei der Auswahl des Personals auf eine entsprechende Qualifizierung geachtet werden und es werden explizit technische Maßnahmen wie Virens Scanner, Firewall und Backups gefordert. Auch die Verschlüsselungstechnologie wird konkreter beschrieben, eine minimale Schlüssellänge in Bits ist angegeben.

Ebene

Auch bei diesem Gütesiegel werden webshop-spezifische organisatorische und technische Anforderungen beschrieben.

Voraussetzungen

Das Gütesiegel „s@fer shopping“ kann nur von Webshops erworben werden, alternativ gibt es aber noch ein Zertifikat für Webseiten.

Prüfung

Die Konformität wird mittels einer Prüfung festgestellt, die aus drei Komponenten besteht: Einer Online-Prüfung, einem Security-Check und einem Audit vor Ort.

Die Online-Prüfung analysiert zunächst die Webseiten des Shops und führt typische Benutzer-Aktionen wie Suchvorgänge und Bestellungen durch. Der Security-Check erfolgt auch online, hier werden mit verschiedenen Portscannern und Skripts die aus dem Internet erreichbaren technischen Komponenten

⁶ <http://www.trustedshops.de/shopbetreiber/shoploesungen.html>, aufgerufen am 04.08.2010.

⁷ 2.2 von http://www.safer-shopping.de/fileadmin/dateien/PDFs/Anforderungen_Shopsb2c.pdf, aufgerufen am 15.09.2010.

überprüft, also beispielsweise Webserver, Webapplikationen und Firewalls. Der Audit vor Ort prüft hauptsächlich Anforderungen zur Organisation, zur Datensicherheit und zum Datenschutz, außerdem werden Prozesse wie die Abwicklung von Bestellungen angeschaut. Die Ergebnisse werden dokumentiert und dem Unternehmen bereit gestellt.

Bei bestandener Prüfung gilt das ausgestellte Zertifikat drei Jahre lang, wobei jährliche Überwachungsaudits durchgeführt werden. Vor Ende der drei Jahre ist es möglich, durch einen Wiederholungsaudit die Gültigkeit des Zertifikats um weitere drei Jahre zu verlängern.

Aufwand und Kosten

Die Kosten für die Zertifizierung sind abhängig von Faktoren wie der Größe der Infrastruktur, allerdings lässt sich einem Informationsprospekt⁸ entnehmen, dass man von Kosten in vierstelliger Höhe ausgehen kann. Ein Verantwortlicher der TÜV Süd AG macht in einem Interview⁹ detailliertere Angaben: Die Prüfung dauert in der Regel vier bis fünf Tage, zusätzlich muss mit einer Vorbereitungszeit gerechnet werden. Die Kosten für die Prüfung belaufen sich auf mindestens 4.500 Euro.

Nutzen und Anpassbarkeit

Bei diesem Gütesiegel ist die Prüfung vor Ort hervorzuheben, durch die garantiert wird, dass auch Sicherheitsanforderungen wie Zutrittskontrollen erfüllt sind. Auch hier sind die Anforderungen vorgegeben, eine Anpassung ist daher kaum möglich, aber auch nicht erforderlich.

5.1.3 Internet Privacy Standards

Das Gütesiegel „internet privacy standards“ (ips) der datenschutz cert GmbH besitzt von allen untersuchten Gütesiegeln die meisten und ausführlichsten Anforderungen. Bisher sind 21 Zertifikate¹⁰ vergeben worden, darunter auch ein Webshop. Der Katalog der Qualitätskriterien¹¹ ist unterteilt in insgesamt neun Module, die an verschiedene Funktionen, die dem Verbraucher geboten werden, angelehnt sind. Sie beschreiben neben den Anforderungen auch für verschiedene Umsetzungsgrade die Maßnahmen, die in einem Unternehmen umgesetzt sein sollten.

Das Modul „M 1 Info-Abruf“ beschreibt beispielsweise Anforderungen an das Bereitstellen von Informationen auf Webseiten und das Modul „M 5 e-Government“ legt fest, wie Gütesiegel-konforme Webseiten von Behörden aufzubauen sind.

Für Webshops sind die Module „M 1 Info-Abruf“, „M 4 Individual-Dienstleistung“, „M 7 Verbraucherschutz“ und „M 8 Datenschutzmanagement“ von Bedeutung. Die für die Betrachtung der IT-Sicherheit relevanten Anforderungen befinden sich hauptsächlich im Modul „M 8 Datenschutzmanagement“, welches neben Datenschutz-Anforderungen auch die Datensicherheit berücksichtigt. Auch das Modul „M 4 Individual-Dienstleistung“ enthält Sicherheitsanforderungen.

Der Unterpunkt „technisch-organisatorische Sicherheitsmaßnahmen“ im Modul „M 8 Datenschutzmanagement“ beschreibt unter anderem Anforderungen zum Schutz der Infrastruktur und orientiert sich dabei an der Anlage zu §9 des Bundesdatenschutzgesetzes (siehe Abschnitt 3.2.1). Thematisiert werden verschiedene Kontrollen: Unter dem Oberbegriff „Zutrittskontrolle“ werden alle Maßnahmen gegen unberechtigten physischen Zugriff auf Daten zusammengefasst. Der Punkt „Zugangskontrolle“ beschreibt Anforderungen an die Protokollierung der Zugriffe und Passwortvorgaben, technische Vorgaben wie Firewalls und ihre Konfiguration sowie Schutz gegen Viren und trojanische Pferde. Die Zugriffskontrolle beinhaltet ein Berechtigungskonzept und Authentifizierungsmöglichkeiten. Des Weiteren wird noch überprüft, ob E-Mails verschlüsselt und Datenübertragungen protokolliert werden, um die unbemerkte, ungewollte Verbreitung von Daten zu verhindern. Auch weiterführende Methoden wie Backup-Systeme

⁸ http://www.safer-shopping.de/fileadmin/dateien/PDFs/Prospekt_safer-shopping.pdf, aufgerufen am 04.08.2010.

⁹ <http://www.it-business.de/partnerzone/ebusiness/web/articles/259538/index3.html>, aufgerufen am 19.09.2010.

¹⁰ <http://www.datenschutz-cert.de/zertlisten/index.html>, aufgerufen am 07.10.2010.

¹¹ http://www.datenschutz-cert.de/kriterien/ips_katalog1.html, aufgerufen am 16.08.2010.

werden aufgegriffen.

Ebene

Die Anforderungen des Gütesiegels ips bestehen aus technischen Vorgaben und allgemeineren organisatorischen Richtlinien.

Voraussetzungen

Das Gütesiegel kann für verschiedene Online-Inhalte vergeben werden, unter anderem für eCommerce-, eGovernment- und einfache Informations-Webseiten.

Prüfung

Die Evaluierung wird von einem lizenzierten ips-Auditor¹² durchgeführt, meist nur über das Internet. Ist das Verwalten von personenbezogenen Daten eine wesentliche Funktion des geprüften Systems, wird auch das Datenschutzmanagement vor Ort überprüft. Nach dem Audit können gegebenenfalls festgestellte Mängel beseitigt wurden, darauf folgt eine Abschlussprüfung. Das Prüfungssystem ist komplexer als bei anderen Gütesiegeln: Für jede Anforderung werden je nach Umsetzungsgrad zwischen 0 und 3 Punkte vergeben. So wird eine Durchschnittspunktzahl für jedes Modul berechnet. Die einzelnen Module werden von einem Gutachter unterschiedlich gewichtet, sodass die Punktzahl dieser Module gewichtet in die Endpunktzahl einfließt. Die Voraussetzung zur Erlangung des Gütesiegels ist eine gewichtete Durchschnittspunktzahl größer als 2,0.

Sicherheitsrelevante Zertifikate wie ISO 27001 oder IT-Grundschutz können beim Audit berücksichtigt werden. Im Audit-Report wird eine Empfehlung ausgesprochen, die von der Zertifizierungsstelle der datenschutz cert GmbH überprüft wird. Bei einem begründeten Einwand besteht hier die Möglichkeit, das Zertifikat entgegen der Empfehlung des Auditors nicht zu erteilen.

Das Zertifikat ist zwei Jahre gültig, wobei nach einem Jahr ein Überwachungsaudit stattfindet. Eine Rezertifizierung ist möglich und im Vergleich zur Erstprüfung vereinfacht.

Bei Veränderung der geprüften Funktionen kann das Gütesiegel schon vor Ablauf der zwei Jahre ungültig werden.

Aufwand und Kosten

Abhängig von Faktoren wie der Unternehmensgröße dauert eine Evaluierung 2-4 Arbeitstage, die jeweils mit 1.150 € berechnet werden. Zusätzlich kostet die Zertifizierung bis zu 750 €¹³.

Nutzen und Anpassbarkeit

Die Qualitätskriterien beinhalten unter anderem wichtige Regeln zur Zutritts- und Zugriffskontrolle. Ohne die Vor-Ort-Prüfung, die in der Regel nicht durchgeführt wird, können die Maßnahmen zur Zutrittskontrolle aber nicht überprüft werden. Das Gütesiegel ist für Webshops konzipiert, eine Anpassung ist daher nicht erforderlich.

5.1.4 EHI Geprüfter Online-Shop

Das Gütesiegel „EHI Geprüfter Online-Shop“ wird vom EHI Retail Institute vergeben, einem Zusammenschluss von Handelsunternehmen und Branchenverbänden. Es wurden 421 Shops zertifiziert¹⁴. Das Gütesiegel ist an das euro-label angeschlossen, eine Kooperation von sechs nationalen europäischen Gütesiegel-Anbietern. Diese Vereinigung hat einen Europäischen Verhaltenskodex (Code of Conduct)¹⁵ aufgestellt, der aber keine Anforderungen an Maßnahmen zum Schutz der Infrastruktur hat und nur die

¹² http://www.datenschutz-cert.de/download/ips/RegisterAudatoren_ips.pdf, aufgerufen am 16.08.2010.

¹³ <http://www.datenschutz-cert.de/download/ips/VergabeNutzungsbedingungen.pdf>, aufgerufen am 07.10.2010.

¹⁴ <http://www.shopinfo.net/zertifizierte-shops/index.html>, aufgerufen am 12.10.2010.

¹⁵ <http://www.euro-label.com/kodex/index.html>, aufgerufen am 11.10.2010.

Gewährleistung der Vertraulichkeit der Daten fordert, ohne konkrete Wege zum Erreichen dieses Ziels aufzuzeigen.

Die Prüfkriterien¹⁶ des Gütesiegels gehen jedoch über diesen Verhaltenskodex hinaus. Sie sind in 17 Paragraphen unterteilt. § 17 beschäftigt sich mit der IT-Sicherheit und fordert ein „angemessenes Sicherheitskonzept“, welches die Sicherheit von Kundendaten, den Schutz der Systeme und Verfahren gegen unberechtigten Zugriff und die verschlüsselte Übertragung von Zahlungsinformationen sicherstellt. Es wird spezifiziert, dass diese Verschlüsselung eine Schlüssellänge von 1024 Bit für den Schlüsseltausch und starke Kryptographie (als Beispiel wird Triple DES 168/112 Bit angegeben) einsetzen muss. Es darf keine unverschlüsselte Übertragung von Zahlungsinformationen stattfinden.

Ebene

Für eine erfolgreiche Zertifizierung werden sowohl technische Maßnahmen wie das sicherheitsorientierte Überprüfen von Datenverbindungen als auch Prozessanalysen, beispielsweise durch Testbestellungen, durchgeführt.

Voraussetzungen

Dieses Gütesiegel wird nur an Webshops vergeben.

Prüfung

Nach der ausschließlich über das Internet durchgeführten Prüfung, bei der ein Prüfbericht in Form einer Checkliste erstellt wird, bleibt dem Webshop Zeit, Verbesserungen umzusetzen, die in einer Endkontrolle überprüft werden. Der Bericht enthält Vorschläge zur Beseitigung der Mängel und unterstützt so das zu zertifizierende Unternehmen.

Das Zertifikat ist ein Jahr gültig, danach muss eine Nachprüfung vorgenommen werden. Auch hier gibt es die Möglichkeit, nicht erfüllte Anforderungen nachträglich umzusetzen.

Aufwand und Kosten

Laut Webseite¹⁷ kann der gesamte Ablauf von der Prüfung bis zur Vergabe des Gütesiegels unter sehr guten Bedingungen drei Wochen dauern.

Die Kosten für das Gütesiegel sind abhängig vom Umsatz des Unternehmens und liegen bei 750-2.800 € im Jahr (siehe Tabelle 5.1).

Jahresumsatz	jährliche Kosten für das Gütesiegel
bis 250.000 €	750 €
bis 500.000 €	850 €
bis 1.000.000 €	950 €
bis 2.500.000 €	1.200 €
bis 5.000.000 €	1.800 €
bis 10.000.000 €	2.200 €
mehr als 10.000.000 €	2.800 €

Tabelle 5.1: Kosten für das EHI-Gütesiegel¹¹

Nutzen und Anpassbarkeit

Eine erfolgreiche Zertifizierung liefert anhand von mehreren überprüften Kriterien eine Aussage über das momentane Sicherheitsniveau und beinhaltet Vorschläge zur Verbesserung von Schwachstellen. Das Gü-

¹⁶ <http://www.shopinfo.net/haendler/kriterien/index.html>, aufgerufen am 11.10.2010.

¹⁷ <http://www.shopinfo.net>, aufgerufen am 11.10.2010.

¹⁸ <http://www.shopinfo.net/haendler/kosten/index.html>, aufgerufen am 07.10.2010.

tesiegel ist speziell auf Webshops abgestimmt, eine Anpassbarkeit ist aufgrund der festgelegten Kriterien nicht möglich, aber auch nicht notwendig.

5.2 Weitere Webshop-Gütesiegel

Neben den von der Initiative D21 empfohlenen Gütesiegeln, die auch in Tests (zum Beispiel in einem Gütesiegel-Test der Zeitschrift Computer-Bild 03/2009) gut abgeschnitten haben, gibt es noch weitere Gütesiegel, die allerdings weniger Sicherheitsanforderungen haben und hier nur im Überblick vorgestellt werden.

Das Internetgütesiegel Sicher & Seriös

Das Internetgütesiegel wurde bisher an 835 Shops verliehen (Stand: 12.08.2010). Laut Aussage der Webseite¹⁹ sind die Prüfungskriterien²⁰ an die Kriterien der Initiative D21 angelehnt und um weitere ergänzt. Eine offizielle Konformität wird nicht angestrebt. Die Anlehnung beinhaltet jedoch keinesfalls eine vollständige Übernahme der Kriterien, unter dem Punkt „Datenschutz und Datensicherheit“ finden sich lediglich einige Anforderungen aus dem Bundesdatenschutzgesetz wie der Grundsatz der Datenvermeidung. Es werden keine Aussagen über IT-Sicherheit gemacht, lediglich bei der Beschreibung der Zahlungsarten und -bedingungen ist gefordert, dass ein gültiges SSL-Verschlüsselungssystem vorhanden sein muss²¹. Außerdem wird gefordert, dass die Zugangsdaten zur Shop-Administration regelmäßig geändert werden sollen (also mindestens zur jährlichen Neu-Zertifizierung).

Zur Prüfung wird die Webseite des zu prüfenden Shops besichtigt. Abweichungen oder Verbesserungsmöglichkeiten werden dem Webshop dann mitgeteilt. Nachdem diese beseitigt sind, nimmt eine externe Rechtsanwaltskanzlei die Prüfung vor und tätigt dabei auch eine Testbestellung. Nach erfolgreichem Abschluss wird das Gütesiegel verliehen, zur Aufrechterhaltung sind jährliche Überprüfungsaudits notwendig.

Das Gütesiegel ist auf Verbraucherfreundlichkeit ausgerichtet, der Sicherheitsaspekt wird allerdings vernachlässigt. Das Gütesiegel sagt demnach fast nichts über das Niveau der IT-Sicherheit aus.

Sicher einkaufen im Netz

Der Fokus des Gütesiegels „Sicher einkaufen im Netz“²² liegt auf der Sicherheit des Kunden: Es wird überprüft, ob der Shop sich an die geltenden Gesetze hält und die Identität von Shop und Betreiber bestätigt. Auf der Webseite gibt es keinerlei Auskunft darüber, wie viele Gütesiegel bisher bereits verliehen wurden, auf Anfrage wurde mitgeteilt, dass bisher erst „wenige“ Shops zertifiziert sind. In Bezug auf technische Sicherheit finden sich in den 50 Qualitätskriterien²³ nur zwei Punkte: Zahlungsinformationen verschlüsselt übertragen werden und Kundendaten müssen durch ein Passwort geschützt werden. Der Shop muss sich des weiteren noch dazu verpflichten, die Gesetze zum Datenschutz zu befolgen.

Nach einer Prüfung der Qualitätskriterien in der Erstprüfung wird das Gütesiegel bei Konformität zu den Anforderungen verliehen. Es gibt verschiedene Abstufungen: Das Siegel kann in Bronze, Silber und Gold verliehen werden, dabei steigt die Anzahl der zu erfüllenden Anforderungen (so muss bei Gold der Bestelleingang sofort per e-mail bestätigt werden). Neben der Prüfung über das Internet findet eine telefonische Verifikation sowie eine Überprüfung von Dokumenten wie der Gewerbeanmeldung statt, die dem Gütesiegel-Anbieter zugesendet werden müssen. Nach der Zertifizierung folgen in unregelmäßigen Abständen weitere Prüfungen. Kunden des Webshops können über ein Formular auf der Webseite des Gütesiegels Feedback geben, welches Kontrollen durch den Prüfer zur Folge haben kann. Das Gütesiegel ist für 1 Jahr gültig, die tatsächliche Laufzeit kann aber vom Webshop bestimmt werden und 3, 6 oder

¹⁹ <http://www.internetsiegel.net/html/shopbetreiberinfo.html>, aufgerufen am 12.08.2010.

²⁰ <http://www.internetsiegel.net/Pruefungskriterien-detail.pdf>, aufgerufen am 12.08.2010.

²¹ <http://www.internetsiegel.net/PDF/Pruefungskriterien.pdf>, aufgerufen am 12.08.2010.

²² <http://www.tdssl.de/>, aufgerufen am 07.10.2010.

²³ <http://www.tdssl.de/qualitaetskriterien.htm>, aufgerufen am 07.10.2010.

12 Monate betragen.

Das Gütesiegel prüft in technischer Hinsicht lediglich, ob eine verschlüsselte Verbindung zum Kunden besteht. Eine Zertifizierung sagt nichts über das Sicherheitsniveau eines Shops aus.

User-friendly Online Shop

„User-friendly Online Shop“²⁴ ist mehr ein Gutachten als ein Gütesiegel und konzentriert sich ausschließlich auf die Benutzbarkeit des Shops. Sicherheitsüberprüfungen werden daher überhaupt nicht vorgenommen.

Bonicert

Das Gütesiegel „Bonicert geprüfter Shop“²⁵ konzentriert sich bei der Prüfung auf die Verbraucherrechte. So findet sich in den Qualitätskriterien²⁶ neben Datenschutzbestimmungen nur die Anforderung, dass Zahlungsinformationen SSL-verschlüsselt übertragen werden sollen. Nach der Prüfung besteht Gelegenheit, Verbesserungen umzusetzen. Dann wird das Zertifikat verliehen, welches 12 Monate gültig ist. Es sagt aber nichts über das IT-Sicherheitsniveau aus.

Chip/Xonio Online-Shop-Zertifikat

Dieses Gütesiegel kann nur von Webshops erlangt werden, die am kostenpflichtigen Preisvergleich von Chip.de teilnehmen. Die Qualitätskriterien²⁷ fordern die Einhaltung der datenschutzrechtlichen Bestimmungen sowie den Einsatz von Verschlüsselung und eines IT-Sicherheitskonzept, welches nicht näher definiert ist.

5.3 Datenschutz-Gütesiegel

Die folgenden Gütesiegel konzentrieren sich ausschließlich auf Datenschutz-Aspekte. Auch in den vorigen Gütesiegeln gab es schon Datenschutz-Anforderungen, „internet privacy standards“ weist sogar schon durch den Namen darauf hin. Neben dem engerem Fokus sind die in diesem Kapitel vorgestellten Gütesiegel allgemein auf technische Systeme anwendbar und daher nicht wie die vorigen auf Webshops spezialisiert.

5.3.1 ULD-Datenschutz-Gütesiegel

Das Datenschutz-Gütesiegel des unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH) bietet eine Zertifizierung für sicherheitskritische Produkte und ist auf Datensicherheit und Datenschutz fokussiert. Momentan sind Gütesiegel an 32 Produkte vergeben²⁸, zum Beispiel für Verfahren zur Datenvernichtung. Aktuell gibt es keine Webshops mit ULD-Datenschutz-Gütesiegel.

Der Anforderungskatalog für die Zertifizierung [8] orientiert sich stark an den rechtlichen Vorgaben, sowohl am bundesweit geltenden Bundesdatenschutzgesetz als auch an Gesetzen des Landes Schleswig-Holstein, zum Beispiel dem Landesdatenschutzgesetz oder der schleswig-holsteinischen Datenschutzverordnung (DSVO). Er ist unterteilt in ein allgemeines Anforderungsprofil und ein Anforderungsprofil für Protokolldaten.

Das allgemeine Anforderungsprofil, dessen Struktur in Tabelle 5.2 dargestellt ist, gilt für personenbezogene Daten (Primärdaten).

²⁴ <http://www.shoplue.com/cms/website.php?id=/de/index/shop-usability-gutachten.htm>, aufgerufen am 09.10.2010.

²⁵ <http://www.bonicert.de/>, aufgerufen am 11.10.2010.

²⁶ http://www.bonicert.de/files/BC-Quali_v2.0.pdf, aufgerufen am 11.10.2010.

²⁷ http://www.chip.de/artikel/CHIP-Xonio-Online-GmbH-Shop-Zertifizierung-2_12866303.html, aufgerufen am 11.10.2010.

²⁸ <https://www.datenschutzzentrum.de/guetesiegel/register.htm>, aufgerufen am 01.10.2010.

Komplex	Beschreibung
1	Grundsätzliche technische Ausgestaltung von IT-Produkten
2	Zuverlässigkeit der Datenverarbeitung
3	Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen
4	Rechte der Betroffenen

Tabelle 5.2: Die Bestandteile des allgemeinen Anforderungsprofils des Anforderungskatalogs [8]

- Der erste Komplex konzentriert sich vor allem auf die Grundsätze der Datensparsamkeit und Transparenz, es sollen also nur die wirklich benötigten Daten gespeichert werden und die Verarbeitung der Daten muss für Anwender und Betroffene nachvollziehbar sein.
- Komplex 2 bezieht sich hauptsächlich auf die Einhaltung der Datenschutzgesetze und -richtlinien, die alle Phasen der Datenverarbeitung betreffen.
- Der dritte Komplex ist technischer, hier wird geprüft, ob die Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität) erreicht worden sind. Unter anderem werden dafür Firewalls, Virenschutz und Verschlüsselungsverfahren untersucht. Auch die Zugangs- und Zugriffskontrollen zu Datenträgern müssen die Datenschutz-Regelungen einhalten.
- Komplex 4 enthält Anforderungen zu den Rechten der Benutzer. Sie müssen Auskunft über die von ihnen gespeicherten Daten bekommen und Löschungen bzw. Sperrungen der Daten veranlassen können.
Da Protokolldaten (Sekundärdaten) weniger sicherheitskritisch sind, besteht das Anforderungsprofil für Protokolldaten nur aus ausgewählten Anforderungen des allgemeinen Anforderungsprofils.

Ebene

Sowohl organisatorisch als auch technisch werden Maßnahmen gefordert, um den Datenschutz zu gewährleisten.

Voraussetzungen

Das Datenschutz-Gütesiegel kann für Hardware, Software und Verfahren zur Datenverarbeitung vergeben werden. Es besteht die Voraussetzung, dass das zu zertifizierende Produkt geeignet ist, um von öffentlichen Stellen genutzt zu werden²⁹. Da dies aber ein weit gefasster Begriff ist, der unter anderem auch Krankenhäuser und Universitäten umfasst, ist die Zertifizierung einer Webshop-Software möglich. Die Zielgruppe des Produkts darf primär Unternehmen oder Privatleute umfassen, muss also nicht für öffentliche Stellen hergestellt worden sein.

Prüfung

Die Prüfung besteht aus einer Evaluations- und Zertifizierungsphase. Zunächst findet eine Evaluation durch einen vom ULD SH akkreditierten Prüfer³⁰ statt. In der Zertifizierungsphase überprüft das ULD SH das fertige Gutachten auf Plausibilität und stellt so sicher, dass die Methodik eingehalten wurde und die Argumentation schlüssig ist.

Das Datenschutz-Gütesiegel wird für 2 Jahre vergeben, danach kann es mit einem vereinfachten Rezertifizierungsverfahren verlängert werden. Dieses wird auch bei größeren Änderungen während der 2 Jahre

²⁹ <https://www.datenschutzzentrum.de/faq/guetesiegel.htm#2>, aufgerufen am 27.09.2010.

³⁰ <https://www.datenschutzzentrum.de/guetesiegel/registga.htm>, aufgerufen am 07.10.2010.

angewendet.

Aufwand und Kosten

Laut Datenschutz-Gütesiegel-FAQ³¹ dauert eine Prüfung mehrere Monate. Allein die Plausibilitätsprüfung durch das ULD SH kostet 1280 bis 3840 Euro, je nach Komplexität³², die Prüfer verlangen zusätzlich eine Gebühr.

Nutzen und Anpassbarkeit

Das Datenschutz-Gütesiegel kann nur für einzelne Produkte wie Hardware, Software oder Datenverarbeitungsverfahren vergeben werden, nicht für den ganzen Webshop. Ähnlich wie bei den Common Criteria (siehe Abschnitt 4.8) liegt eine Zertifizierung eher in der Zuständigkeit des Herstellers. Eine Zertifizierung von einzelnen Komponenten wie der Shop-Software ist daher vor allem hilfreich, wenn sie von der KMU selbst entwickelt wurde. Sie bestätigt die Konformität zum Bundesdatenschutzgesetz und zu den Datenschutzrichtlinien von Schleswig-Holstein. Eine Anpassung ist aufgrund der festgelegten Kriterien nicht möglich.

5.3.2 Datenschutz-Gütesiegel der Freien Hansestadt Bremen

Das Datenschutz-Gütesiegel der freien Hansestadt Bremen ist ebenfalls auf den Datenschutz und die Datensicherheit ausgerichtet und wird für 2 Jahre vergeben. Es wurde nach dem Datenschutz-Gütesiegel des unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (siehe Abschnitt 5.3.1) eingeführt und orientiert sich an diesem.

Das Datenschutz-Gütesiegel ist in der Bremischen Datenschutzauditverordnung (BremDSAAuditV)³³ beschrieben, welche laut Quelle seit Anfang 2010 außer Kraft getreten ist. Auf Anfrage wurde jedoch mitgeteilt, dass die Gültigkeit der BremDSAAuditV bis zum 31. Dezember 2014 verlängert wurde. Aufgrund der Einschränkung, dass das Gütesiegel nur an öffentliche Stellen vergeben werden kann, sind bisher nicht viele Zertifizierungen erfolgt (im Jahr 2007 waren es nur zwei³⁴).

Mit dem Auditor zusammen wird eine Vereinbarung über den Ablauf des Audits und Art und Umfang des Verfahrens getroffen (BremDSAAuditV §2 (1)). Es wird ein Datenschutzplan ausgearbeitet, der den aktuellen Stand, die Ziele und ein Datenschutzmanagementsystem beschreibt. Letzteres beschreibt Zuständigkeiten, Arbeitsabläufe und einen Mechanismus, um den Fortschritt zu überwachen und zu dokumentieren.

Ebene

Zum Datenschutz werden technische und organisatorische Maßnahmen gefordert (vgl. BremDSAAuditV §4 (1)).

Voraussetzungen

Der Audit ist öffentlichen Stellen vorbehalten. Es werden „Verfahren mit den dazugehörigen technischen Einrichtungen“ (vgl. BremDSAAuditV §1 (1)) zertifiziert.

Prüfung

Die Prüfung wird von einem durch den Landesbeauftragten für Datenschutz zugelassenen Auditor (beispielsweise datenschutz cert GmbH³⁵, der vom Antragsteller vorgeschlagen werden kann, durchgeführt. Er prüft den Datenschutzplan, kann aber das Verfahren auch selbst besichtigen. Er erstellt ein Gutachten

³¹ <https://www.datenschutzzentrum.de/faq/guetesiegel.htm>, aufgerufen am 27.09.2010.

³² https://www.datenschutzzentrum.de/faq/guetesiegel.htm#7_2, aufgerufen am 27.09.2010.

³³ http://www.datenschutz-bremen.de/pdf/brosch_BremDSAAuditV.pdf, aufgerufen am 27.10.2010.

³⁴ <http://www.senatspressestelle.bremen.de/detail.php?id=1715>, aufgerufen am 07.10.2010.

³⁵ <http://www.datenschutz-cert.de/>, aufgerufen am 07.10.2010.

und muss der öffentlichen Stelle gegebenenfalls Zeit zur Behebung der Beanstandungen geben. Eine Bestätigung durch eine Behörde erfolgt nicht.

Das Gütesiegel ist zwei Jahre gültig, kann aber durch ein vereinfachtes Verfahren verlängert werden.

Aufwand und Kosten

Über Aufwand und Kosten ist nichts bekannt.

Nutzen und Anpassbarkeit

Da das Gütesiegel öffentlichen Stellen vorbehalten ist, kann es für KMU-Webshops nicht angewendet werden.

5.3.3 Europäisches Datenschutz-Gütesiegel

Das Projekt EuroPriSe (European Privacy Seal) der Europäischen Union wurde 2007 mit dem Ziel gestartet, ein europäisches Datenschutz-Gütesiegel zu etablieren, welches die Vereinbarkeit mit dem europäischen Datenschutzrecht bestätigt. Es wurde maßgeblich durch das als Vorbild dienende Datenschutz-Gütesiegel des unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH) beeinflusst, wobei die Kriterien an europaweite Gesetze angepasst wurden.

Das Gütesiegel bescheinigt die Vereinbarkeit des Zertifizierungsgegenstands mit europäischen Datenschutz-Richtlinien, hauptsächlich der Datenschutzrichtlinie der Europäischen Union (Richtlinie 95/46/EG), der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) und den Dokumenten der Artikel 29 Datenschutzgruppe. Eine Konformität wird nicht garantiert, da diese von der Art der Nutzung der zertifizierten Produkte abhängt. Nationale Gesetze der teilnehmenden Staaten werden lediglich berücksichtigt, sind aber nicht bindend (S. 625, [33]). Für die Datensicherheit ist vor allem die integrierte sicherheitstechnische Überprüfung relevant.

Der Aufbau des Kriterienkatalogs³⁶ ist identisch zum ULD-Gütesiegel: Es gibt vier Komplexe, die in kleinere Teilkomplexe aufgeteilt sind.

Der Erste, „Fundamental Aspects of Processing“, untersucht allgemeine Aspekte wie den Grund der Datenspeicherung und die Art der gespeicherten Daten. Hier wird auch die technische Umsetzung der Datenschutz-Grundsätze wie zum Beispiel Datenvermeidung und Transparenz geprüft.

„Legitimacy of Data Processing“ ist der zweite Komplex, er befasst sich mit allen rechtlichen Details wie der Analyse der Rechtsgrundlage, der Rechtmäßigkeit aller Schritte der Datenverarbeitung und der Einhaltung der Datenschutz-Grundsätze.

Der dritte Komplex, „Technical-Organisational Measures: Accompanying Measures for Protection of the Data Subject“, überprüft, ob Zugriffskontrollen und andere technische Maßnahmen zum Schutz der Daten eingeführt worden sind. Auch andere spezifische Schutzmaßnahmen wie Verschlüsselung werden überprüft, diese sind aber nicht für jeden Zertifizierungsgegenstand anwendbar, sodass in diesem Kapitel für jede Anforderung beschrieben ist, welche Vorbedingungen für die Anwendbarkeit erfüllt sein müssen.

Der letzte Komplex trägt den Titel „Data Subjects’ Rights“ und beschäftigt sich mit den durch die Datenschutzrichtlinien definierten Rechte der Personen, deren Daten verarbeitet werden.

Ebene

Wie auch beim ULD-Gütesiegel liegt der Fokus auf dem Datenschutz, sowohl auf technischer als auch auf organisatorischer Ebene.

Voraussetzungen

Das Gütesiegel kann für IT-Produkte und IT-Dienstleistungen vergeben werden und besitzt damit einen größeren Anwendungsbereich als andere Gütesiegel, was sich in generischen Kriterien äußert, die nicht

³⁶ <https://www.european-privacy-seal.eu/criteria>, aufgerufen am 11.10.2010.

als festgelegte Checkliste aufgelistet sind, sondern einen Ermessensspielraum für den Prüfer enthalten.

Prüfung

Genau wie beim Gütesiegel des ULD SH besteht die Prüfung aus einem zweistufigen Verfahren, bei dem zunächst ein akkreditierter Sachverständiger ein Gutachten verfasst, welches dann bei einer der Zertifizierungsstellen eingereicht wird. Sind alle die relevanten Kriterien eingehalten und das Gutachten schlüssig, wird das Gütesiegel vergeben. Es ist für zwei Jahre gültig und kann durch ein Re-Zertifizierungsverfahren erneuert werden.

Aufwand und Kosten

Eine Zertifizierung dauert in der Regel länger als drei Monate³⁷.

Es wird eine Zertifizierungsgebühr erhoben, die aber im Vergleich zu den Kosten für den Gutachter niedrig ausfällt. Letztere sind abhängig von der Komplexität¹⁵.

Nutzen und Anpassbarkeit

Das Gütesiegel ist nicht speziell auf Webshops abgestimmt, wie beispielsweise die D21-Gütesiegel, sondern geeignet für alle technischen Produkte. Dies birgt die Gefahr von zu generellen Anforderungen, die nicht ausreichend auf den konkreten Anwendungsfall abgebildet werden können. Es deckt alle relevanten Kriterien ab, die von europäischen Datenschutzgesetzen gefordert werden, darunter auch Sicherheitsanforderungen.

Eine Anpassung ist aufgrund der festgelegten Kriterien nicht möglich.

³⁷ <https://www.datenschutzzentrum.de/sommerakademie/2008/sak08-bock-probst-europrise.pdf>, aufgerufen am 28.07.2010.

6 Sonstige Sicherheitsüberprüfungen

Neben Standards und Gütesiegeln gibt es noch verschiedene andere Möglichkeiten, die IT-Sicherheit der Infrastruktur zu bewerten.

Grundsätzlich gibt es zwei Ansätze: Entweder die Prüfungen werden intern, das heißt von Mitarbeitern des betroffenen Unternehmens, durchgeführt oder es wird ein externer Dienstleister hinzugezogen.

Letzteres kann durch externe Sicherheits-Audits geschehen. Sie überprüfen die Sicherheit von Systemen, indem die Infrastruktur des Unternehmens, aber auch Prozesse und umgesetzte Maßnahmen analysiert, bewertet und gegebenenfalls mit ein vorgegebenen Wert verglichen werden.

Wenn das Unternehmen seine IT-Sicherheit ohne fremde Hilfe überprüfen will, hat es im Allgemeinen zwei Möglichkeiten, die aber auch kombiniert werden können. Zum Einen sind Fragebögen oder Checklisten verfügbar, durch die eine Einschätzung über den Stand der Sicherheit gewonnen und Problembereiche aufgedeckt werden, zum Anderen gibt es Analyseprogramme, mit deren Hilfe technische Schwachstellen ausfindig gemacht werden können. Auch die zuvor genannten Sicherheits-Audits können intern durchgeführt werden, Voraussetzungen sind dabei aber Auditoren, die über Expertenwissen in dem Gebiet verfügen, aber nicht in die Konzeption und Entwicklung der Sicherheitskomponenten beteiligt sind. Beispielsweise können sich mehrere IT-Abteilungen gegenseitig auditieren - da KMUs aber in der Regel nur eine IT-Abteilung haben, ist dies selten möglich. Daher werden interne Sicherheitsaudits im Weiteren vernachlässigt.

Zur Analyse der Methoden wird das in Abschnitt 1.4 definierte Template verwendet. Zusätzlich werden zu jeder Methode noch mehrere für Webshops geeignete Beispiele aufgelistet.

6.1 Fragebögen und Checklisten

Fragebögen und Checklisten versprechen einen schnellen Überblick über die momentane Situation der IT-Sicherheit. Die zuständigen Mitarbeiter im Unternehmen können sie ohne externe Hilfe in kürzester Zeit durchführen und erhalten dann je nach Konzeption eine Bewertung der IT-Sicherheit oder konkrete Verbesserungsvorschläge.

Ebene

Die Fragen konzentrieren sich in den analysierten Beispielen auf Details zur Infrastruktur und Organisation.

Voraussetzungen

Für die Durchführung sind neben einem fachkundigen Mitarbeiter keine Bedingungen notwendig. Meistens haben die Fragebögen und Checklisten spezielle Zielgruppen und Schwerpunkte, die beachtet werden sollten.

Prüfung

Oft kann die Prüfung innerhalb von wenigen Stunden abgehandelt werden.

Aufwand und Kosten

Die Kosten für die Evaluation bestehen bei kostenlosen Checklisten und Fragebögen nur aus der Arbeitszeit der Mitarbeiter. Der Aufwand für die Umsetzung von empfohlenen Maßnahmen oder Beseitigung der entdeckten Schwachstellen kann schwer verallgemeinert werden. Bei den unten aufgeführten Beispielen dürften sie akzeptabel sein, insbesondere da man davon ausgehen kann, dass einige der Basis-Sicherheitsmaßnahmen in vielen Unternehmen schon umgesetzt sind.

Nutzen und Anpassbarkeit

Nach Abarbeiten des Fragebogens oder der Checkliste sind mögliche Defizite in der Regel erkennbar. Da die Checklisten und Fragebögen aber für möglichst viele Unternehmen gültig sind, können nur allgemeine Fragen gestellt werden. Durch die kurze und oft oberflächliche Prüfung kann man sich selbst bei einem positiven Ergebnis nicht sicher sein, ob alle wesentlichen Gefährdungen durch entsprechende Maßnahmen abgedeckt sind.

IT-Sicherheit für Kleinstunternehmen

Der von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) in Auftrag gegebene und von der hessischen Wirtschaftsförderung HA Hessen Agentur GmbH entwickelte Online-Fragebogen¹ bietet eine einfache Sicherheitsanalyse und einen anschließenden Maßnahmenplan. Er ist in vier Phasen unterteilt (siehe Abbildung 6.1.1).

Phase 1: Risiko-Profil-Auswahl Phase 2: Auswahl kritischer Unternehmenswerte Phase 3: Auswahl der Sicherheitsanforderungen Phase 4: Risiko-Management & Umsetzung
--

Abbildung 6.1.1: Die Phasen des ENISA-Fragebogens für Kleinstunternehmen

Er richtet sich vor allem an Kleinstunternehmen, die als Unternehmen mit bis zu 9 Mitarbeitern und bis zu 2 Mio. Euro Umsatz oder Bilanzsumme definiert werden. Zunächst wird überprüft, ob eine IT-Sicherheitsanalyse eigenständig durchgeführt werden kann oder externe Dienstleister benötigt werden. Darauf folgt anhand eines fünfseitigen Fragebogens („IT-Sicherheits-Check“) eine Ermittlung des aktuellen Sicherheitsniveaus.

In Phase 1 wird durch kurze Fragen zu den wichtigsten Risiken ein einfaches Risikoprofil ermittelt und die kritischen Unternehmenswerte der Kategorien Systeme, Netzwerke, Mitarbeiter und Anwendungen ausgewählt. Diesen werden ein oder mehrere Schutzkriterien (Vertraulichkeit, Verfügbarkeit, Integrität) zugewiesen.

Der Fragebogen erzeugt nun Sicherheitsanforderungen für die ausgewählten Unternehmenswerte und organisatorische Anforderungen, zu denen jeweils Umsetzungsansätze notiert werden sollen.

In der letzten Phase wird geprüft, inwiefern die Anforderungen schon umgesetzt sind („Ja“, „Nein“, „Teilweise“). Danach kann jeder Anforderung eine Priorität („Gering“, „Mittel“, „Hoch“) zugeordnet und eine Maßnahme zur Umsetzung beschrieben werden. Zuletzt wird jeder Anforderung und den zugeordneten Maßnahmen ein Verantwortlicher und ein Meilenstein (Datum) zugewiesen und vermerkt, ob externe Hilfe benötigt wird.

Abschließend sind sowohl der Komplettbericht, aber auch die vorher erstellten Pläne als pdf/xls-Datei aufrufbar.

sicher-im-netz.de

Der Verein „Deutschland sicher im Netz e.V.“ bietet eine Checkliste für Unternehmen an². Hier werden allgemeine Sicherheitsmaßnahmen wie Firewalls, regelmäßiges Updaten der Software sowie die Beschreibung von konkreten Verhaltensweisen, etwa beim Empfang einer e-mail mit verdächtigem Anhang thematisiert. Insgesamt richtet sich das Dokument meistens an den PC-Benutzer, dem mögliche

¹ <http://www.kmu-sicherheit.eu/index.cfm?pid=-1>, aufgerufen am 31.07.2010.

² https://www.sicher-im-netz.de/files/documents/06_01_Checkliste_firmen.pdf, aufgerufen am 30.07.2010.

Bedrohungen und eine angemessene Reaktion darauf beschrieben werden und eher selten an die IT-Sachverständigen einer Firma, zum Beispiel wenn es darum geht, Software bereit zu stellen. Des Weiteren bietet der Verein noch andere Ratgeber an, die die Absicherung eines Unternehmen zum Ziel haben:

- Das „Pocket Seminar IT-Sicherheit“³, welches Teil einer Schriftenreihe der SAP AG ist, richtet sich speziell an kleine und mittlere Unternehmen. Es thematisiert die Sicherheit von einzelnen PCs, Netzwerken und Betriebssystemen, besitzt aber auch einen Teilabschnitt über Internet-Auftritte. Nach jedem Kapitel folgt eine Checkliste, in der die wichtigsten Sicherungsmaßnahmen notiert sind. Die enthaltenen Informationen sind aber recht oberflächlich gehalten, der Fokus liegt auf einem schnellen Überblick über viele Themen.
- Die in Zusammenarbeit mit DATEV entstandene Informationsbroschüre „Sicher im Netz - Leitfaden zum sicheren Umgang mit IT für Unternehmen“⁴ enthält unter anderem ein Unterkapitel „Sicherheitsvorkehrungen“, in dem elementare Bedrohungen und Schutzmaßnahmen aus Sicht der Unternehmen aufgelistet sind.

InfoSurance

Der Verein InfoSurance aus der Schweiz hat ein 10-Punkte-Programm für KMUs entwickelt⁵, das 2009 um 10 weitere Punkte für mehr Vertraulichkeit und Verfügbarkeit ergänzt wurde.

Punkt 1	Erstellen Sie ein Pflichtenheft für IT-Verantwortliche!
Punkt 2	Sichern Sie Ihre Daten regelmässig mit Backups!
Punkt 3	Halten Sie Ihr Antivirus-Programm aktuell!
Punkt 4	Schützen Sie Ihren Internetzugang mit einer Firewall!
Punkt 5	Aktualisieren Sie Ihre Software regelmässig!
Punkt 6	Verwenden Sie starke Passwörter!
Punkt 7	Schützen Sie Ihre mobilen Geräte!
Punkt 8	Machen Sie Ihre IT-Benutzerrichtlinien bekannt!
Punkt 9	Schützen Sie die Umgebung Ihrer IT-Infrastruktur!
Punkt 10	Ordnen Sie Ihre Dokumente und Datenträger!

Abbildung 6.1.2: Die 10 Maßnahmen von InfoSurance für einen wirkungsvollen Grundschutz

Die Punkte bestehen aus Anweisungen, die allgemein gehalten sind und zu den Standard-Sicherheitsmaßnahmen gehören, wie beispielsweise die Einrichtung einer Firewall und eines regelmäßig aktualisierten Antivirenprogramms (siehe Abbildung 6.1.2).

Maßnahmen wie die Verwendung starker Passwörter sind lediglich mit organisatorischem Aufwand verbunden und daher in kleinen Unternehmen schnell umzusetzen.

6.2 Analyseprogramme

Mit Hilfe von Analyseprogrammen können die technischen Komponenten gezielt überprüft werden. Während Anweisungen wie der Befehl nmap (listet die offenen Ports eines Rechners auf) nur einzelne Funk-

³ https://www.sicher-im-netz.de/files/documents/06_02_PocketseminarIT-Secprint.pdf, aufgerufen am 30.07.2010.

⁴ https://www.sicher-im-netz.de/files/documents/unternehmen/DsiN_Unternehmer_Web.pdf, aufgerufen am 30.07.2010.

⁵ http://www.infosurance.ch/site/downloads/merkblaetter/InfoSurance_10_Punkte_Programm_DE.pdf, aufgerufen am 18.07.2010.

tionen bereitstellen, können komplexe Testsammlungen automatisiert mehrere Aspekte der Sicherheit überprüfen. Im Internet finden sich Verzeichnisse mit bekannten Analyseprogrammen⁶.

Analyseprogramme werden oft im Zuge von Penetrationstests (Pen-Tests) eingesetzt, mit denen versucht wird, ohne Berechtigungen in das entsprechende System einzudringen. Es wird also ein Angreifer simuliert, was rechtlich nicht unbedenklich ist, da neben dem Ausspähen von geschützten Daten schon der Besitz von Software, die dies ermöglicht, nach §202c des deutschen Strafgesetzbuches strafbar ist. Für genauere Details über die Rechtslage sei auf ein Dokument des BSI über Penetrationstests verwiesen [18]. Die Durchführung von Penetrationstests birgt die Gefahr, dass Schäden am System entstehen und vertrauliche Daten gelesen werden, der Penetrationstester sollte also vertrauenswürdig sein.

Eine Einteilung der Pen-Tests (vgl. S.85, [11]) kann folgendermaßen vorgenommen werden:

- Beim **Whitebox**-Ansatz werden detaillierte Informationen über das System verwendet. Der nachgebildete Angreifer kennt die interne Struktur und die Anwendungen des Systems.
- Der **Blackbox**-Ansatz simuliert einen Angreifer, der keine beziehungsweise nur öffentlich zugängliche Informationen über das System besitzt. Im Fall von Webshops erkennt der Angreifer beispielsweise anhand des Quelltexts, welches Shop-System eingesetzt wird.

Der Penetrationstester recherchiert zunächst im Internet und findet so erste Informationen. Zusätzlich setzt er Analyseprogramme wie einem Portscanner ein, um möglichst viele Informationen über das Zielsystem zu erfahren (im Fall eines Whitebox-Tests sind diese möglicherweise schon gegeben). Beispielsweise erfährt er, welche Anwendungen in welcher Version auf dem System installiert sind. Durch im Internet frei verfügbare Datenbanken kann er nun spezifische Schwachstellen nachlesen und ausnutzen. Beim Eindringen in durch Passwörter geschützte Bereiche können Wörterbuchattacken verwendet werden. Dazu werden die Wörter aus einem Wörterbuch der Reihe nach oder kombiniert als Passwort ausprobiert.

Ebene

Analyseprogramme decken nur technische Aspekte ab und konzentrieren sich auf die Teile der Infrastruktur, die über das Netzwerk/Internet erreichbar sind.

Voraussetzungen

Die Voraussetzungen sind von Programm zu Programm unterschiedlich, meist ist jedoch nur ein Rechner mit einem bestimmten Betriebssystem erforderlich, der Zugriff auf das Netzwerk und das zu prüfende Objekt (Computer oder Webseite) hat.

Prüfung

Die Prüfung findet durch das Programm statt, benötigt meist eine nur kurze Zeitspanne und liefert dann einen Ergebnisreport.

Aufwand und Kosten

Der Aufwand ist äußerst gering, die Kosten hängen vom benutzten Programm ab. Die unten aufgeführten Beispielen zeigen Programme verschiedener Preisklassen.

Nutzen und Anpassbarkeit

Der Nutzen hängt von den Tests ab, die von den Programmen durchgeführt werden. Generell erfolgt eine einmalige Prüfung auf bekannte Schwachstellen, die eher statisch ist. Wenn Penetrationstests durchgeführt werden, sind Analyseprogramme ein gutes Hilfsmittel. Vollständige Pen-Tests sind aufwändiger und erfordern Expertenwissen über Angriffstechniken, liefern aber auch mehr Schwachstellen als ein Analyseprogramm alleine.

⁶ <http://sectools.org/>, aufgerufen am 15.08.2010.

Eine Anpassbarkeit ist nicht gegeben, da es sich um eine einfache Abarbeitung einer Liste von Tests handelt. In seltenen Fällen ist allerdings das Hinzufügen von weiteren Tests möglich.

SOPHOS

Der „SOPHOS Computer Security Scan“⁷ ist ein netzwerkbasiertes Analyseprogramm, welches bis zu 200 Computer in einem Netzwerk überprüft. Es testet dabei auf gängige Adware und Malware. Zusätzlich gibt es noch den „Sophos Endpoint Assessment Test“⁸, welcher für einen Windows-PC analysiert, ob aktuelle Betriebssystem-, Webbrowser- und Office-Patches installiert sind und ob ein Antivirenprogramm läuft.

Web Security Toolset

Das Web Security Toolset⁹ von German Websecurity bietet eine Reihe von Werkzeugen an, um eine Webseite sicherheitstechnisch zu analysieren. Laut Hersteller werden unter anderem Webanwendungen auf Buffer Overflows, SQL Injection und Cross Site Scripting überprüft. Die Kosten für eine Lizenz betragen 249 Euro und beinhalten ein Jahr Support.

BSI Open Source Security Suite

BSI Open Source Security Suite (BOSS) ist ein Werkzeug zum Überprüfen von Netzwerken und lokalen Rechnern. Die Anwendung ist auf den IT-Grundschutz abgestimmt. BOSS ist mittlerweile in Version 3.0 verfügbar und enthält OpenVAS¹⁰, eine kostenlose Software, die auf dem beliebten, nun separat weiterentwickelten Nessus¹¹ basiert. Nessus wurde in vorigen Versionen von BOSS eingesetzt, ist seit kurzem allerdings keine Open-Source Software mehr. BOSS wird als Live-CD angeboten¹², OpenVAS kann aber auch von der Herstellerhomepage bezogen werden, wobei es sich um eine Software für Linux handelt. Sie ist durch Plug-Ins erweiterbar und ermöglicht so eine Anpassung der Testdurchführung.

6.3 Sicherheits-Audits

Sicherheitsaudits bestehen aus einer einmaligen Prüfung. Im Folgenden liegt der Fokus auf den externen Audits, die von einem Dienstleister durchgeführt werden. Oftmals existiert ein Kriterienkatalog, der überprüft wird. Dies kann mit Hilfe von Befragungen der Mitarbeiter, Auswertung von Unternehmensdaten wie Protokollen und veröffentlichten Richtlinien oder durch Tests der Infrastruktur passieren. Je nach Audit können technische und/oder organisatorische Sicherheitsmaßnahmen geprüft werden. Oft werden bei technischen Überprüfungen Penetrationstests durchgeführt, bei denen versucht wird, über ein Netzwerk in das System einzudringen und so Sicherheitslücken ausfindig zu machen (siehe auch Abschnitt 6.2). Meistens bestehen die Audits also aus einer Kombination von Checklisten und Analyseprogrammen.

⁷ <http://www.sophos.de/products/free-tools/sophos-computer-security-scan.html>, aufgerufen am 30.07.2010.

⁸ <http://www.sophos.de/products/free-tools/sophos-endpoint-assessment-test.html>, aufgerufen am 30.07.2010.

⁹ <http://www.german-websecurity.com/de/produkte/web-security-toolset/produktinformationen/uebersicht/>, aufgerufen am 30.07.2010.

¹⁰ <http://www.openvas.org/>, aufgerufen am 30.07.2010.

¹¹ <http://www.nessus.org/>, aufgerufen am 30.07.2010.

¹² https://www.bsi.bund.de/cln_156/ContentBSI/Themen/ProdukteTools/BOSS/BSIOSS.html, aufgerufen am 01.08.2010.

Ebene

Je nach Audit kann eine eher technische und/oder organisatorische Überprüfung der IT-Sicherheit stattfinden.

Voraussetzungen

Außer dem Budget gibt es keine generellen Voraussetzungen für Sicherheitsaudits. Einige der unten genannten Beispiele erfordern eine Internetverbindung und sind speziell für Webseiten konzipiert.

Prüfung

Die Prüfung findet entweder vor Ort oder über das Internet statt. Typisch ist die kurze Dauer, nach einer Woche bei ausführlicheren und einem Tag bei einfacheren Audits liegt das Ergebnis vor.

Aufwand und Kosten

Die Kosten für den Sicherheitsaudit sind je nach Größenordnung unterschiedlich. Die unten aufgeführten Beispiele enthalten sowohl kostenlose Angebote als auch Audits, die einen vierstelligen Betrag kosten. Der Aufwand für das Unternehmen ist gering, da die Durchführung des Audits und die Auswertung vom Auditor übernommen wird. Daher entfällt eine Einarbeitungszeit und es ist kein Expertenwissen notwendig, lediglich die Mitarbeiter, die den Auditor unterstützen, müssen Arbeitszeit aufwenden.

Nutzen und Anpassbarkeit

Der Nutzen hängt von der Vollständigkeit des Kriterienkatalogs ab. Für Unternehmen, die keine Erfahrungen im Bereich der IT-Sicherheit haben und keine Mitarbeiter dafür einstellen können, bietet ein Sicherheitsaudit oft die einzige Chance, die Infrastruktur trotzdem auf Basis von Expertenwissen sicherheitstechnisch bewerten zu lassen. Der Audit wird in der Regel so durchgeführt, dass er die Eigenschaften des Unternehmens wie Größe und Infrastruktur berücksichtigt.

Trusted Shops Security Audit

Der Trusted Shops Security Audit¹³ ist ein speziell auf Webshops abgestimmter Sicherheits-Audit und wird von Trusted Shops GmbH, dem Anbieter des zuvor vorgestellten Gütesiegels (siehe Abschnitt 5.1.1) angeboten. Der Fokus der Prüfung liegt auf den technischen und organisatorischen Methoden, die die IT-Sicherheit gewährleisten sollen. Sie bietet - verglichen mit dem Basis-Audit von Trusted Shops - eine genauere Betrachtung von möglichen Schwachstellen: Beispielsweise wird überprüft, ob der Shop verwundbar durch Angriffe wie Cross-Site Scripting und Content Spoofing ist. Datenverbindungen zum Kunden werden analysiert, unter anderem sollte die Registrierung eines Benutzers per HTTPS erfolgen, da persönliche Kundendaten übermittelt werden. Außerdem werden Vorgaben, die die Sicherheit betreffen, überprüft, zum Beispiel die Minimallänge bei der Wahl des Kundenpassworts.

Die (öffentlich nicht zugänglichen) Prüfkriterien sind in drei Risikoklassen¹⁴ aufgeteilt (III(muss), II(soll), I(kann)), wobei die Kriterien der höchsten Risikoklasse unbedingt erfüllt sein müssen, um eine gewisse Sicherheit des Webshops zu garantieren. Jedes Kriterium hat eine Punktzahl, sodass sich durch die Summe der erfüllten Anforderungen eine Gesamtpunktzahl ergibt, aufgrund der eine Einschätzung über die Absicherung des Webshops vorgenommen wird. Nach der Prüfung listet ein Audit-Report die gefundenen Schwachstellen auf und gibt Vorschläge für Gegenmaßnahmen.

Der Security-Audit kostet einmalig 1490 €.

¹³ <http://www.trustedshops.de/shopbetreiber/security-audit.html>, aufgerufen am 01.08.2010.

¹⁴ http://www.trustedshops.de/shopbetreiber/pdf_download/security-audit_auszug.pdf, aufgerufen am 06.10.2010.

German Web Security

German Web Security¹⁵ ist ein kostenloser Dienst, der Webseiten auf Sicherheitslücken prüft. Die detaillierte Auswertung des Ergebnisses ist allerdings kostenpflichtig.

Die Prüfung konzentriert sich auf bekannte Sicherheitslücken und Angriffe, vor allem gegen Formulare und Eingabefelder (zum Beispiel SQL-Injection oder Buffer-Overflows). Des Weiteren werden Zugriffsversuche auf versteckte Dateien unternommen. Auf der Homepage findet sich eine ausführliche Beschreibung aller Tests¹⁶.

Eine detaillierte Auswertung des Scans kostet 99 €.

Bei erfolgreicher Prüfung, d.h. Durchführung eines kompletten Scans ohne kritische und mittlere Sicherheitslücken, kann eine Art Zertifikat, welches die Überprüfung der Webseite bescheinigt, ausgestellt werden.

secure-it.nrw

Die vom Bundesland Nordrhein-Westfalen unterstützte Initiative „secure-it.nrw“ bot für kleine und mittlere Unternehmen eine kostenlose „Basisprüfung IT-Sicherheit“ an. Dieser Sicherheitscheck wurde bis 31.12.2009 gefördert und ist nun eingestellt.

Um diesen Audit durchführen zu lassen, mussten sich die Unternehmen registrieren. Es durften nur KMUs teilnehmen, insbesondere die Zahl der PC-Arbeitsplätze musste bei 5-100 liegen. Die kostenlose Prüfung orientierte sich am IT-Grundschutz des BSI, war aber weniger umfangreich. Auch hier lag der Fokus auf der technischen Ebene.

Ein Auditor arbeitete innerhalb von circa vier Stunden einen Fragebogen mit 130 Fragen ab, die die Infrastruktur, Anwendungen und übergreifende Aspekte berücksichtigten¹⁷.

Anschließend bekam das auditierte Unternehmen Empfehlungen für das weitere Vorgehen.

Quick-Check IT-Sicherheit

Der Verein „ruhr networker e.V.“, der sich aus verschiedenen Unternehmen aus dem Bereich IT und Medien zusammensetzt, bietet einen Quick-Check IT-Sicherheit¹⁸ an.

Bei diesem Test schickt das Unternehmen zunächst einen ausgefüllten zweiseitigen Fragebogen an den Verein. Thematisch deckt er sowohl Fragen zur IT-Sicherheits-Organisation, als auch zu technischen Maßnahmen, Schulungen und Outsourcing ab, bleibt dabei aber immer sehr allgemein.

Danach findet ein kostenfreies Beratungsgespräch mit einem der Mitgliedsunternehmen¹⁹ statt, welches ca. 30 Minuten dauert.

Der Aufwand für diese kurze Überprüfung fällt durch das Ausfüllen von 19 Fragen und dem halbstündigen Gespräch extrem gering aus. Danach besteht die Möglichkeit, weitere (kostenpflichtige) Dienstleistungen der Mitgliedsunternehmen in Anspruch zu nehmen, unter denen sich einige IT-Beratungen befinden.

¹⁵ <http://www.german-websecurity.com>, aufgerufen am 11.10.2010.

¹⁶ <http://www.german-websecurity.com/de/produkte/web-scan-service/weitere-information/testmethoden-im-detail/>, aufgerufen am 01.08.2010.

¹⁷ [http://www.newmedianrw.de/media2/site/index.php?id=73&tx_ttnews\[tt_news\]=52061](http://www.newmedianrw.de/media2/site/index.php?id=73&tx_ttnews[tt_news]=52061), aufgerufen am 30.07.2010.

¹⁸ http://www.ruhr-networker.de/quick_its.0.html, aufgerufen am 01.08.2010.

¹⁹ <http://www.ruhr-networker.de/mitglieder.0.html>, aufgerufen am 07.10.2010.

7 Analyse

In den vorangegangenen Kapiteln wurde eine Übersicht über verschiedene Methoden zur Evaluierung der IT-Sicherheit gegeben. Dabei wurde deutlich, dass einige Methoden eher organisatorische Maßnahmen zur Überprüfung und Umsetzung verwenden, andere eher eine technik-fokussierte Herangehensweise nutzen. Die Abbildungen 7.0.1 und 7.0.2 zeigen eine grobe Einordnung der untersuchten Methoden. Die Audits sind jeweils mittig eingeordnet, wobei es natürlich vom Dienstleister und den Wünschen des auditierten Unternehmens abhängt, ob sich die Durchführung auf technische oder organisatorische Details konzentriert.

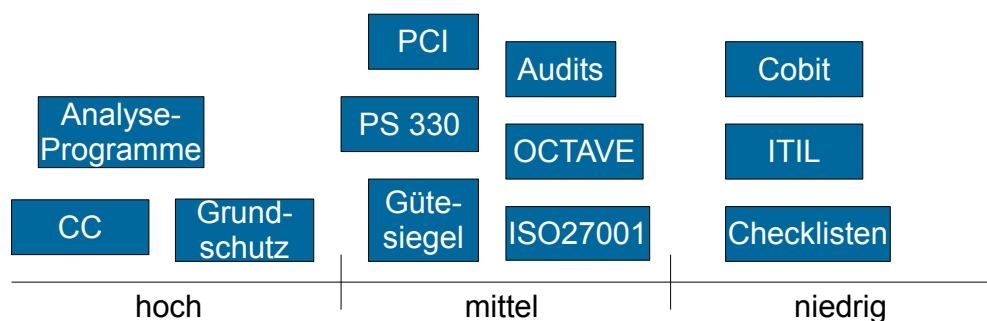


Abbildung 7.0.1: Grobe Einordnung der Methoden anhand der technischen Fokussierung

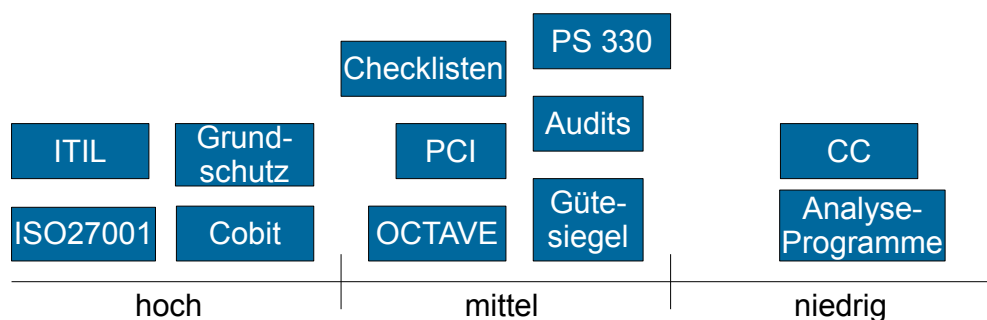


Abbildung 7.0.2: Grobe Einordnung der Methoden anhand der organisatorischen Fokussierung

Die verschiedenen vorgestellten Ansätze und Methoden haben unterschiedliche Ziele und auch unterschiedliche Anwendungs- und Wirkungsbereiche: Während ISO 27001 ein Managementsystem auf organisatorischer Ebene bereit stellt, mit dem die Sicherheit nachhaltig implementiert werden soll, überprüft ein Analyseprogramm einen bestimmten Webserver auf technische Schwachstellen. Die beiden Methoden schließen sich aber nicht aus, zur vollständigen Evaluation muss die Sicherheit auf allen Ebenen überprüft werden. So kann durch das Managementsystem der Webserver als Wert des Unternehmens identifiziert werden, der geschützt werden muss. Daraufhin kann eine Überprüfung seiner Schwachstellen angeordnet werden, beispielsweise durch eine Analyseprogramm.

Neben den unterschiedlichen Zielen sind vor allem die benötigten Ressourcen ein wichtiges Entscheidungskriterium für KMUs. Die Frage ist daher auch, wie viel der Webshop in die Sicherheit investieren kann und will. Zur Veranschaulichung sind daher die Methoden nach den wichtigsten Nebenkriterien

Aufwand, Kosten und benötigtes Wissen analysiert und jeweils in drei Kategorien (niedrig, mittel, hoch) eingeteilt. Diese grobe Aufteilung ist nötig, da besonders Kosten und Aufwand sehr stark von der Komplexität der Infrastruktur abhängen.

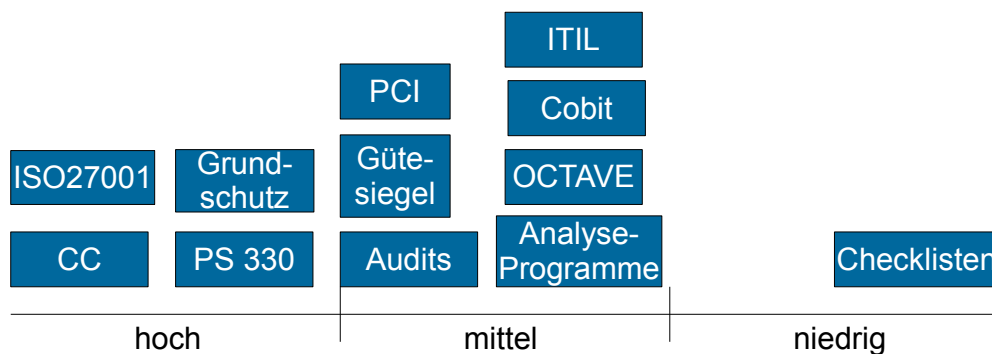


Abbildung 7.0.3: Einordnung der Methoden nach dem Kriterium „Kosten“

Die Abbildung 7.0.3 zeigt die Einordnung bezüglich der Kosten der Methoden. Während die teuren, aufwändigeren Standards wie ISO 27001 und Common Criteria hohe Kosten verursachen und für KMU-Webshops daher schwer finanzierbar sind, ist die finanzielle Belastung der Kategorien „mittel“ und „niedrig“ tragbar: Die Risikoanalyse nach OCTAVE benötigt beispielsweise lediglich ein Team von erfahrenen Mitarbeitern und Analyseprogramme kosten nur bei der Anschaffung Geld. Standards ohne Prüfungen und Zertifizierungen wie ITIL und Cobit verursachen lediglich durch benötigte Arbeitszeit und Infrastruktur Kosten. Checklisten und Fragebögen sind oft kostenlos im Internet verfügbar und daher am günstigsten.

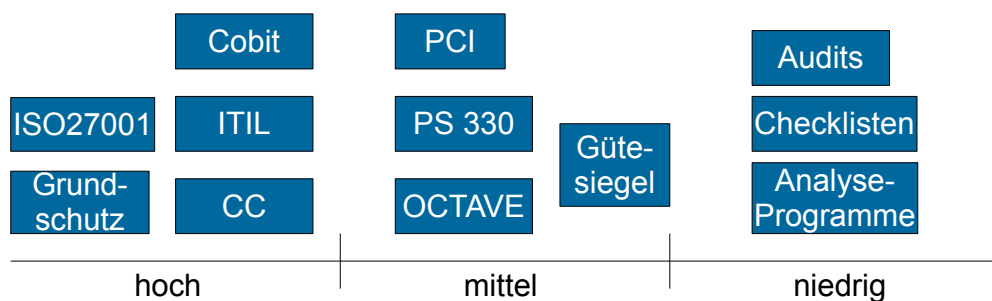


Abbildung 7.0.4: Einordnung der Methoden nach dem Kriterium „Aufwand“

Bei der Betrachtung des Aufwands (Abbildung 7.0.4) zeigt sich, dass die Standards, die hohe Kosten verursachen, meistens auch einen hohen Aufwand erfordern (zum Beispiel ISO 27001, Common Criteria, IT Grundschutz). Überschaubare Standards wie PCI und Octave haben einen geringeren, aber nicht zu vernachlässigenden Aufwand. Bei den Audits oder auditähnlichen Methoden wie PS 330 (Audit durch Wirtschaftsprüfer) oder den Gütesiegeln ist der Aufwand mittel bis niedrig einzuschätzen. Checklisten sind meistens schnell abgearbeitet und Analyseprogramme laufen größtenteils automatisch ab, daher ist der Aufwand gering.

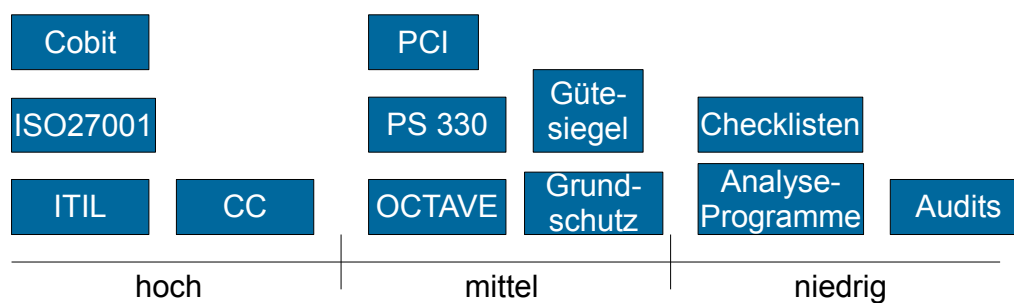


Abbildung 7.0.5: Einordnung der Methoden nach dem Kriterium „benötigtes Wissen“

Abbildung 7.0.5 ordnet die Methoden nach dem benötigten Wissen, welches bei den Mitarbeitern des Unternehmens vorhanden sein muss. Audits werden von Experten durchgeführt, da aber - wie in Kapitel 6.3 erwähnt - der Fokus auf externen Audits liegt, benötigen die Mitarbeiter kein Expertenwissen. Auch die Abarbeitung von Checklisten und die Durchführung von Prüfungen mit Analyseprogrammen ist ohne tiefere Kenntnisse im Bereich IT-Sicherheit möglich. Die gegebenenfalls notwendigen Nachbesserungen bei Gütesiegeln und die Durchführung der Standards erfordern mehr Wissen.

7.1 Eignung von Standards

In Kapitel 4 wurden verschiedene Standards mit unterschiedlichen Zielsetzungen vorgestellt. Grundsätzlich sind sie im Vergleich zu den anderen Methoden aufwändiger und benötigen mehr Ressourcen. Im Folgenden wird jeder einzelne Standard auf seine Anwendbarkeit für KMU-Webshops analysiert:

- Die ISO 27001 Norm bietet viele Vorteile wie internationale Anerkennung und die mögliche Integration von weiteren Standards, aber die Zertifizierung ist zu teuer und die Vorgehensweise zu komplex. Es sind außerdem erfahrene Mitarbeiter notwendig, um anhand der abstrakten Ziele, die der Standard vorgibt, passende Maßnahmen auszuwählen, welche auf die in Abschnitt 3.2.3 beschriebenen Gefährdungen abgestimmt sind.
- IT-Grundschutz ist ein aufwändiger Standard, der die technische und organisatorische Ebene abdeckt und die IT-Sicherheit nicht nur analysiert, sondern auch verbessert. Wenn nach der Evaluierung eine umfangreiche Verbesserung angestrebt wird, so bietet IT-Grundschutz eine Methodik, die an vielen Stellen vereinfacht werden kann und zudem einen Leitfaden enthält, der im Vergleich zu anderen Standards weniger Expertenwissen erfordert, da die Maßnahmen zum größten Teil vorgegeben sind. Bisher ist allerdings kein Webshop mit IT-Grundschutz zertifiziert¹, was darauf schließen lässt, dass der Aufwand dennoch zu hoch ist.
- Der Payment Card Industry Standard wird meist umgesetzt, weil es die Verarbeitung von Kreditkartendaten erfordert. Werden diese Daten nicht in irgendeiner Weise verarbeitet, ist der Standard nicht verpflichtend, kann nicht vollständig umgesetzt und vor allem nicht zertifiziert werden, da sich die Anforderungen auf den Schutz der Kreditkartendaten beziehen. Wenn Kreditkartendaten verarbeitet werden, bietet der Standard einen guten Basis-Schutz und ist in der Lage, einige der in Abschnitt 3.2.3 beschriebenen Gefährdungen (beispielsweise einen Malware-Angriff oder das Abhören des Kommunikationskanals) zu verhindern. Dies erfordert allerdings einen größeren Aufwand. Die Pflicht zur Umsetzung des Standards kann umgangen werden, indem die Speicherung und Verarbeitung der Kreditkartendaten ausgelagert wird.

¹ https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Zertifikate/iso27001zertifikate_node.html, aufgerufen am 05.10.2010.

- Die Risikoanalyse nach OCTAVE, besonders die Anwendung von OCTAVE-S, bietet einem Webshop einen schnellen Überblick über die Risiken. Mit den Informationen aus der Analyse kann die IT-Sicherheit bewertet werden. Für eine Evaluierung ist der Standard daher sehr gut geeignet, vorausgesetzt, entsprechende Ressourcen - vor allem ein Team von erfahrenen Mitarbeitern - können bereitgestellt werden.
- Der service-orientierte ITIL-Standard ist aufwändig und schlecht auf Webshops anwendbar, da sich die dort vorgestellten Maßnahmen kaum auf die Bestell- und Liefervorgänge abbilden lassen. Außerdem spielt der Sicherheitsaspekt keine große Rolle, sodass sich dieser Standard nicht gut für die Evaluation der IT-Sicherheit eignet.
- Cobit bietet eine allgemeines Management der IT und geht nur nebenher auf die Sicherheit ein. Der durch die Implementierung der Kontrollen auf verschiedenen Ebenen entstehende Mehraufwand ist für Webshop-KMUs nicht tolerierbar, auch wenn die für IT-Sicherheit angelegten Kontrollen eine dauerhafte Rückmeldung über das Sicherheitsniveau geben würden.
- Der Prüfungsstandard IDW PS 330 ist eher zweckgebunden, er prüft die rechnungsrelevanten Systeme auf Risiken, die zu einer Verfälschung der Bilanzen führen könnten. Durch die Analyse der bisher umgesetzten Maßnahmen soll ein externer Wirtschaftsprüfer die Sicherheit beurteilen. Die Testmethoden sind nicht im Detail festgelegt, sodass schwierig zu beurteilen ist, ob die Gefährdungen mit Hilfe des Standards entdeckt werden. Fraglich ist allerdings, ob eine XSS-Attacke, die den Inhalt der Webseite bei einem Kunden ändert, schon als Risiko für die Rechnungslegung eingestuft und berücksichtigt wird.
- Die Common Criteria eignen sich nur bedingt zur Evaluation der IT-Sicherheit eines Webshops, da sie in der Regel auf einzelne Komponenten angewendet werden. Schon die Evaluation einzelner Schlüsselkomponenten wie der Webshop-Software ist für KMUs sehr aufwändig und zu teuer. Des Weiteren wird der Standard eher von Herstellern genutzt, die ihr Produkt bewerten wollen und sich dadurch einen Wettbewerbsvorteil erhoffen. Der Webshop ist aber kein Hersteller des Webserver oder der Komponenten, er kann allenfalls seine Shop-Software selbst entwickelt haben. Da diese aber in der Regel nicht weiterverkauft wird, sondern nur für den Eigenbedarf genutzt wird, sind die Kosten viel höher als der Nutzen, sodass sich die Common Criteria für die Evaluation der IT-Sicherheit von Webshops nicht eignen.

Ausgehend von den Eigenschaften von KMUs wie dem beschränkten Finanzierungsspielraum und wenigen Mitarbeitern, erfordern die aufwändigen Standards wie ISO 27001, IT-Grundschutz, Cobit und Common Criteria zur Evaluierung der IT-Sicherheit zu viele Ressourcen. Andere Standards wie ITIL und der Prüfungsstandard IDW PS 330 sind nicht auf die IT-Sicherheit der ganzen Infrastruktur fokussiert. Lediglich der PCI-Standard, sofern er angewendet werden muss, und die Risikoanalyse nach OCTAVE sind zur Evaluation der IT-Sicherheit geeignet, wobei OCTAVE ein erfahrenes Team von Mitarbeitern benötigt und PCI etwas aufwändig ist, sodass keine uneingeschränkte Empfehlung für jeden Webshop ausgesprochen werden kann.

7.2 Eignung von Gütesiegeln

In den Abbildungen 7.0.1 und 7.0.2 wurden die Gütesiegel zusammengefasst, da sie nahezu identische Kriterien prüfen. Daher liefert auch eine Zertifizierung bei allen eine ähnliche Auskunft über die Sicherheit des Systems. Tabelle 7.1 visualisiert die für die IT-Sicherheit wichtigsten Übereinstimmungen bei den Qualitätskriterien der Anbieter. Bemerkenswert ist, dass alle auf Webshops spezialisierten Online-Gütesiegel die Datenschutzbestimmungen überprüfen. Das Erlangen eines Datenschutzgütesiegels, das keinerlei Spezialisierung auf Webshops bietet, hat demnach bezüglich der IT-Sicherheit keinen Mehrwert. Die nicht von D21 empfohlenen Gütesiegel „sicher & seriös“ (s&s), „Sicher einkaufen im Netz“ (s.e.i.N.),

„Bonicert“ (Bc) und „Chip/Xonio Online-Shop-Zertifikat“ (CX) bieten kaum Sicherheitskriterien und sind daher für eine Überprüfung der IT-Sicherheit nicht empfehlenswert. „User-friendly Online Shop“ wurde erst gar nicht in die Tabelle aufgenommen, weil es keinerlei Sicherheitsüberprüfungen enthält.

Da zwar die recht allgemein verfassten Kriterien für die Gütesiegel öffentlich sind, jedoch nicht die Evaluationsmethoden, ist es schwer, die Gütesiegel genau nach ihrem Nutzen zu priorisieren. Die von der Initiative D21 empfohlenen Gütesiegel überprüfen die meisten Sicherheitskriterien und sind als nahezu gleichwertig zu betrachten.

Kriterium	D21	TS	S@fer S.	ips	ehi	s&s	s.e.i.N.	Bc	CX	uld	euro- prise
IT-Sicherheits- konzept	x	x	x	x	x				x		
Verschlüsselungs- verfahren	x	x	x	x	x	x	x	x	x	x	x
Zutrittskontrolle		x	x	x						x	x
Zugriffskontrolle	x	x	x	x	x		x			x	x
Virens Scanner			x	x						x	
Integration v. Standards				x							
Einhaltung Datenschutz- richtlinien	d. x	x	x	x	x		x	x	x	x	x

Tabelle 7.1: Vergleich der Gütesiegel

Allgemein haben die Gütesiegel (mit Ausnahme der Datenschutz-Gütesiegel) den großen Vorteil, dass sie auf Webshops zugeschnitten sind. Die Überprüfung durch die entsprechenden Auditoren kann als spezieller Sicherheitsaudit verstanden werden. Bei bestandener Prüfung wird ein Zertifikat vergeben, das die Konformität öffentlich bescheinigt und verkaufsfördernd wirkt². Jedoch gibt es nicht nur bei den Kriterien selbst, sondern auch bei den Überprüfungen große Unterschiede zwischen den einzelnen Gütesiegeln. So testen viele von ihnen nur über das Internet. Das „s@fer-shopping“ Gütesiegel von Tüv Süd beinhaltet hingegen auch einen Vor-Ort-Check, sodass auch Kriterien wie die physische Sicherheit der Daten überprüft werden können. Trotzdem kann selbst diese ausführlichere, aber dennoch nur wenige Tage dauernde Prüfung nicht jede Schwachstelle eines Webshops aufdecken: Beispielsweise wurden XSS-Angriffe erfolgreich gegen Webshops mit „s@fer shopping“ Gütesiegel durchgeführt³. Insbesondere viele der in Abschnitt 3.2.3 aufgeführten technischen Schwachstellen bleiben trotz Prüfung verborgen. Ein Abhören des Kommunikationskanals ist allerdings nicht mehr möglich, auch der physische Zugriff wird bei vielen Gütesiegeln stark erschwert. Obwohl viele Webshops Kreditkartenzahlung anbieten und viele der analysierten Gütesiegel auf Webshops spezialisiert sind, gibt es keinen Bezug zum Kreditkartenstandard PCI.

Trotz Spezialisierung auf Webshops testen Gütesiegel nur wenige der Gefährdungen. Die Datenschutzbestimmungen werden jedoch von allen Gütesiegeln überprüft. Durch die nicht öffentlichen Evaluationsmethoden ist es schwer, die Qualität der Zertifizierung abzuschätzen, da nicht klar ist, wie sie ihre Qualitätskriterien überprüfen. Daher erhält ein Webshop mit der Zertifizierung durch ein Gütesiegel in

² eResult-Studie „Relevanz von Gütesiegeln“:

http://www.eresult.de/studien_artikel/forschungsbeitraege/guetesiegel.html, aufgerufen am 19.09.2010.

³ <http://www.netzwerk-internet.de/web-security/artikel/d/truegerische-sicherheit-warum-sie-trotz-tuev-siegel-nicht-jedem-web-shop-trauen-koennen.html>, aufgerufen am 19.09.2010.

erster Linie ein Vertrauensgewinn bei den Kunden, aber keine genaue Aussage über die Absicherung seiner Infrastruktur.

7.3 Eignung von sonstigen Sicherheitsüberprüfungen

Die Überprüfung der Sicherheit durch Audits, Checklisten und Fragebögen sowie Analyseprogrammen verursacht den geringsten Aufwand, führt allerdings auch zu keiner Zertifizierung. Besonders für einen Webshop mit wenig Wissen im Bereich IT-Sicherheit ist ein externer Sicherheitsaudit die einfachste Möglichkeit, sein Sicherheitsniveau zu evaluieren. Die Qualität der Überprüfung ist abhängig vom Auditor, daher sollte dieser sorgfältig gewählt sein. Ein erfahrener Audit-Dienstleister kann durch eine Kombination von Penetrationstests und Interviews mit Mitarbeitern theoretisch alle in Abschnitt 3.2.3 vorgestellten Gefährdungen erkennen. Durch den dafür notwendigen Aufwand würde ein solcher Audit allerdings teuer sein.

Die Bearbeitung von Checklisten und Fragebögen ist hingegen günstiger, hängt aber stark von der Qualität des Fragebogens und vom Kenntnisstand der Mitarbeiter ab. Meistens werden in Fragebögen eher allgemeine Gefährdungen überprüft, sodass trotzdem viele der Gefährdungen aus Abschnitt 3.2.3 unerkannt bleiben. Bei Einhaltung der Punkte von den Checklisten kann zum Beispiel ein Malware-Angriff verhindert werden (indem ein aktuelles Antiviren-Programm installiert wird). Aufgrund des geringen Aufwands sind Fragebögen und Checklisten eine gute Möglichkeit, um die grundlegenden Sicherheitsaspekte zu überprüfen.

Analyseprogramme zeichnen sich durch einmalige Kosten (Anschaffungspreis) und eine meist einfache Bedienung aus. Aufgrund der vielen verschiedenen angebotenen Programme kann dies nicht generalisiert werden: Die BSI Open Source Security Suite ist beispielsweise weniger komfortabel in der Bedienung als kommerzielle Vertreter, kostet dafür aber kein Geld. Analyseprogramme sind geeignet, um technische Schwachstellen aufzudecken: So können gute Programme viele der in Abschnitt 3.2.3 gezeigten Angriffe, beispielsweise SQL-Injections, DoS-Attacken oder das Abhören des Kommunikationskanals, erkennen. Sie können allerdings nicht überprüfen, ob ein physischer Zugriff auf die Infrastruktur möglich ist.

Der Nachteil aller diese Sicherheitsmaßnahmen ist, dass sie nicht auf eine kontinuierliche Überprüfung ausgelegt sind. Zur dauerhaften Aufrechterhaltung der Sicherheit sollte bei Anwendung einer dieser Methoden daher ein Plan ausgearbeitet werden, der eine Wiederholung dieser Sicherheitsüberprüfungen vorsieht. Für die Überprüfung der technischen Angriffe sind Audits bzw. für erfahrenere Mitarbeiter Analyseprogramme ein sehr nützliches Werkzeug, für die anderen Gefährdungen müssen andere Maßnahmen gefunden werden. Fragebögen und Checklisten prüfen, ob die grundlegenden Sicherheitsmaßnahmen umgesetzt wurden und sind daher wichtig. Sie alleine helfen allerdings wenig gegen zielgerichtete Angriffe aus dem Internet.

7.4 Ergebnis der Analyse

Die Analyse hat gezeigt, dass keine der Methoden uneingeschränkt empfehlenswert für die Evaluation der IT-Sicherheit von KMU-Webshops ist. Die Wahl der Methode hängt von mehreren Parametern ab: Entscheidend ist, ob Mitarbeiter mit Wissen über IT-Sicherheit verfügbar sind, wie viel Geld ausgegeben werden kann und wie viel Aufwand investiert werden soll. Zusätzlich spielt es eine Rolle, ob die Überprüfung einmalig oder regelmäßig stattfinden soll.

Wegen der geringen Ressourcen, die zur Verfügung stehen, können keine umfangreichen Maßnahmen umgesetzt werden. Daher eignen sich viele der Standards aufgrund ihres Aufwands nicht, andere haben einen anderen Fokus und sind daher ungeeignet. Stattdessen kann es für kleine Webshops gut sein, einen inkrementellen Ansatz anzuwenden: Zunächst können durch Fragebögen und Checklisten, die nichts kosten und nur einen geringen Aufwand verursachen, grundsätzliche Sicherheitsmaßnahmen überprüft werden. So wird bereits sichergestellt, dass einige der vorgestellten Gefährdungen (siehe

Abschnitt 3.2.3) wie Malware überprüft werden können. Darauf können dann weitere, komplexere Kontrollen erfolgen.

Für die technische Überprüfung bieten sich vor allem Analyseprogramme an: Sie können bei geringem Aufwand und einmaligen Anschaffungskosten viele der technischen Schwachstellen einer Webseite (zum Beispiel Formulare, die anfällig für SQL-Injections sind) aufdecken. Das Risiko der Gefährdungen kann verringert werden, indem der Webshop etablierte Webshop-Software einsetzt statt eigene zu entwickeln, da diese meist schon ausreichend getestet worden ist und Sicherheitsfunktionen enthält.

Wenn keine Mitarbeiter mit Expertenwissen oder keine Zeit für eigene Maßnahmen vorhanden ist, können Gefährdungen mittels eines externen Audits überprüft werden. Außer den Kosten werden hierfür kaum Ressourcen benötigt. Ein Audit bietet sich auch an, um nach Überprüfung der grundsätzlichen Sicherheitsmaßnahmen das System auf komplexere Gefährdungen zu untersuchen. Sofern ein Team mit Erfahrung im IT-Sicherheitsbereich verfügbar ist, kann eine Risikoanalyse nach OCTAVE-S durchgeführt werden, die ebenfalls zum Ziel hat, weitere Gefährdungen auf technischer und organisatorischer Ebene aufzudecken. Wenn der PCI-Standard angewendet werden muss (bei der Verarbeitung von Kreditkartendaten), bietet er sinnvolle Sicherheitsüberprüfungen, die zusätzliche Gefährdungen ermitteln können, sich aber zum Teil mit den in den Fragebögen und Checklisten aufgelisteten Anforderungen überschneiden.

Gütesiegel beinhalten keine vollständige Prüfung der IT-Sicherheit, decken aber rechtliche Aspekte wie die Datenschutzbestimmungen ab und sind wegen ihrer Marketing-Seiteneffekte beliebt. Die Gütesiegel unterscheiden sich in ihrer Qualität, sodass die richtige Wahl des Gütesiegels entscheidend ist. Die weniger angepassten Datenschutz-Gütesiegel sind für Webshops eher nicht zu empfehlen.

Bei der Wahl der Methode kommt es auch darauf an, ob nur eine einmalige Bestimmung des Sicherheitsniveaus oder eine kontinuierliche Überprüfung gewünscht ist. Beispielsweise können Audits bei einer einmaligen Kontrolle günstiger sein, bei einer dauerhaften Überprüfung kann aber ein Risikomanagementsystem nach OCTAVE-S weniger Kosten verursachen, auch wenn vorher eine Schulung der Mitarbeiter durchgeführt werden muss.

8 Fazit und Ausblick

In dieser Arbeit wurden zunächst die Eigenschaften von KMUs und der Aufbau von Webshops beschrieben. KMUs haben nur geringe finanzielle Mittel und im Vergleich zu größeren Unternehmen weniger Mitarbeiter, die selten in Themen wie IT-Sicherheit spezialisiert sind. Die Infrastruktur von Webshops besteht aus Software- und Hardwarekomponenten, deren Verfügbarkeit ständig gewährleistet sein muss, um die Geschäftstätigkeit zu erhalten. Ausfälle werden nicht nur durch technische Fehler, sondern vor allem durch Gefährdungen aus dem Internet verursacht. Eine Sicherheitsbetrachtung ergab, dass die Webshops durch verschiedene Angriffe gefährdet sind.

Es wurden verschiedene Methoden zur Evaluierung der IT-Sicherheit analysiert: bekannte Standards der IT-Sicherheit, Gütesiegel sowie Sicherheitsaudits, Analyseprogramme, Checklisten und Fragebögen. Neben allgemeinen Daten, Ebene, Voraussetzungen und Prüfung der Methoden wurden Kriterien wie Aufwand, Kosten, Nutzen und Anpassbarkeit berücksichtigt.

Die anschließende Analyse ergab, dass bei der Wahl der Methode die Kosten, der Aufwand sowie das Wissen der Mitarbeiter eine Rolle spielt. Standards sind oft zu aufwändig und zu teuer für kleinere und mittlere Webshops. Lediglich das nicht zertifizierbare Vorgehensmodell nach OCTAVE-S ist mit Hilfe von Expertenwissen umsetzbar. Der Kreditkarten-Standard PCI muss bei Verarbeitung der Kreditkartendaten berücksichtigt werden. Er umfasst sinnvolle Sicherungsmaßnahmen, ohne die Kreditkarten-Verarbeitung sind aber Teile des Standards nicht umsetzbar.

Des Weiteren ist die geplante Anzahl der Sicherheitsüberprüfungen zu berücksichtigen: Bei dauerhafter Überprüfung der IT-Sicherheit kann es sinnvoller sein, ein Überwachungssystem - beispielsweise in Form eines Risikomanagements mit OCTAVE-S - zu implementieren, während bei einem einmaligen Check ein externer Sicherheitsaudit einen geringeren Aufwand bedeutet, besonders wenn wenig Expertenwissen im Bereich IT-Sicherheit vorhanden ist. Für einen langfristigen Überblick über das Sicherheitsniveau ist es jedoch wichtig, die Sicherheitsüberprüfungen regelmäßig durchzuführen und auch auf veränderte Rahmenbedingungen anzupassen.

Grundsätzlich ist es für kleine Webshops zu empfehlen, zunächst durch die im Internet verfügbaren Fragebögen und Checklisten die Basis-Sicherheit zu überprüfen und anschließend weitere Maßnahmen durchzuführen. Für die technische Überprüfung bieten sich Analyseprogramme an, die Einhaltung der Datenschutzbestimmungen können durch Gütesiegel bescheinigt werden. Webshops, die über keinerlei Wissen im Bereich IT-Sicherheit verfügen, können mit Hilfe von externen Sicherheitsaudits eine komfortable Überprüfung des Sicherheitsniveaus erreichen. Letzteres ausgenommen, erfordern alle Methoden ein Mindestmaß an Wissen über IT-Sicherheit. Als Alternative bietet sich für den uninteressierten und unfachkundigen Webshop-Betreiber daher nur das Outsourcing der Infrastruktur an, welches die Verantwortung für die IT-Sicherheit zum Outsourcing-Dienstleister verlagert.

Es wurde gezeigt, dass es derzeit keine optimale Methode zur Evaluierung der IT-Sicherheit gibt, die für alle KMU-Webshops geeignet ist. Die Wahl der Methode hängt von den Ressourcen ab, die der Webshop bereitstellen kann. Einige Methoden wie die aufwändigen Standards konnten jedoch als unpassend ausgeschlossen werden, andere - zum Beispiel die Evaluierung durch Checklisten und Fragebögen - sind für jeden Webshop durchführbar und liefern erste Erkenntnisse über das Sicherheitsniveau. Im Vergleich zu den aufwändigeren Methoden ist ihre Aussagekraft aber eher gering.

Für eine vollständige Evaluation muss auf verschiedene Methoden gleichzeitig zurückgegriffen werden. Selbst Gütesiegel, die den Anspruch haben, auf Webshops abgestimmt zu sein, kontrollieren die Einhaltung der Datenschutzbestimmungen und das grundlegende IT-Sicherheitskonzept, erfassen aber keine Schwachstellen im Programmcode der Webseiten. Zur Analyse dieser Schwachstellen müssen Webshops auf Analyseprogramme zurückgreifen.

Wünschenswert wäre ein Gütesiegel-Anbieter, der sich nicht nur auf die Kundensicherheit in Form von korrekten AGBs und Erfüllung der Datenschutzgesetze konzentriert, sondern explizit auch komplexe-

re technische Anforderungen in seine Qualitätskriterien aufnimmt und diese überprüft. Beispielsweise könnte ein Schwachstellen-Check anhand der in Abschnitt 3.2.3 vorgestellten Liste der kritischsten Schwachstellen in Web-Applikationen [34] durchgeführt werden. Außerdem würde eine genauere Beschreibung der Prüfmethoden dazu führen, dass sowohl Webshops als auch Verbraucher die Auswirkungen eines Gütesiegel-Zertifikats auf die Sicherheit besser einschätzen könnten.

Literaturverzeichnis

- [1] Christopher Alberts, Audree Dorofee, James Stevens und Carol Woody: *Introduction to the OCTAVE Approach*. Carnegie Mellon Software Engineering Institute, August 2003.
- [2] Corinne Alexander und Maria I. Marshall: *The Risk Matrix: Illustrating the Importance of Risk Management Strategies*. Journal of Extension, 2006.
- [3] Michael Bächle und Frank R. Lehmann: *E-Business - Grundlagen elektronischer Geschäftsprozesse im Web 2.0*. Oldenbourg Wissenschaftsverlag, 2010, ISBN 978-3-486-58362-5.
- [4] BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. und DIN Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik und Anwendungen (NIA): *Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk*, August 2009.
- [5] Steven Cook: *A Web Developer's Guide to Cross-Site Scripting*. SANS Institute, Januar 2003.
- [6] Symantec Corporation: *State of Enterprise Security 2010*. 2010. http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf , aufgerufen am 12.10.2010.
- [7] Initiative D21: *D21 - Qualitätskriterien für Internet-Angebote*. 2007. http://www.foehlich.de/guetesiegel/docs/D21_Qualitaetskriterien_2007.pdf , aufgerufen am 13.09.2010.
- [8] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH*, August 2005.
- [9] Vassilis Dimopoulos, Steven Furnell, Murray Jennex und Ioannis Kritharas: *Approaches to IT Security in Small and Medium Enterprises*. 2004.
- [10] Christos Douligeris und Aikaterini Mitrokotsa: *DDoS attacks and defense mechanisms: classification and state-of-the-art*. Computer Networks, Vol. 44:643–666, April 2003.
- [11] Claudia Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg, 2005, ISBN 3-486-57676-3.
- [12] European Opinion Research Group EEIG: *European Union Public Opinion On Issues Relating To Business To Consumer E-Commerce - Executive Summary*. März 2004. http://ec.europa.eu/consumers/topics/btoc_ecomm.pdf , zuletzt aufgerufen am 09.10.2010.
- [13] Hans Peter Fröschle und Susanne Strahringer: *IT Governance*. dpunkt-Verlag, 2006, ISBN 3-89864-382-4.
- [14] Corporate Trust Business Risk & Crisis Management GmbH: *Studie: Gefahrenbarometer 2010 Sicherheitsrisiken für den deutschen Mittelstand*. 2010. <http://www.corporate-trust.de/studie/Gefahrenbarometer2010.pdf> , aufgerufen am 11.10.2010.
- [15] William G.J. Halfond, Jeremy Viegas und Allesandro Orso: *A Classification of SQL Injection Attacks and Countermeasures*. März 2006.
- [16] Gerrit Heinemann: *Der neue Online-Handel - Erfolgsfaktoren und Best Practices*. Gabler Verlag, 2010, ISBN 978-3-8349-1804-8.
- [17] Fachausschuß für Informationstechnologie (FAIT) des IDW: *Entwurf IDW Prüfungsstandard: Abschlußprüfung bei Einsatz von Informationstechnologie (IDW EPS 330)*. Juli 2001.

-
- [18] Bundesamt für Sicherheit in der Informationstechnik: *Studie Durchführungskonzept für Penetrationstests*. November 2003. https://www.bsi.bund.de/cae/servlet/contentblob/487300/publicationFile/\30674/penetrationstest_pdf.pdf , aufgerufen am 10.10.2010.
- [19] Bundesamt für Sicherheit in der Informationstechnik: *IT-Sicherheitsmanagement und IT-Grundschutz*. Bundesanzeiger Verlag, 2005, ISBN 3-89817-547-2.
- [20] IT Governance Institute: *COBIT 4.1*. <http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx> , aufgerufen am 01.10.2010.
- [21] IT Governance Institute: *COBIT 4.1 Excerpt*. <http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx> , aufgerufen am 01.10.2010.
- [22] Projektgruppe IT Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung: *IT-Sicherheitskriterien im Vergleich*. Initiative D21, Dezember 2001.
- [23] Markus Kaufmann und Stefan Cheridito (Zürcher Hochschule Winterthur): *Kleine und mittelgroße Unternehmen und ihre IT-Infrastruktur: Eine Analyse*. 2007.
- [24] Heinrich Kersten, Jürgen Reuter und Klaus Werner Schröder: *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*. Vieweg Verlag, 2008, ISBN 978-3-834-8017-84.
- [25] David Kluge und Samuel Sambasivam: *Formal Information Security Standards in German Medium Enterprises*. CONISAR: The Conference on Information Systems Applied Research, November 2008.
- [26] Jens Koenig: *Ein Informationssystem für das strategische Management in KMU*. Josef Eul Verlag, September 2004. ISBN 3-89936-281-0.
- [27] Mitja Kolsek: *Session Fixation Vulnerability in Web-based Applications*. ACROS Security, Dezember 2002.
- [28] Europäische Kommission: *Die neue KMU-Definition - Benutzerhandbuch und Mustererklärung*. 2005, ISBN 92-894-7907-8.
- [29] Michael Kresse und Markus Bause: *learnIT!Lv3*. Servview GmbH, 2008, ISBN 978-3-9810-9778-8.
- [30] PCI Security Standards Council LLC: *Anleitung und Richtlinien zum PCI-DSS-Selbstbeurteilungs-Fragebogen, v1.2*. 2008.
- [31] PCI Security Standards Council LLC: *PCI DSS Requirements and Security Assessment Procedures, v1.2.1*. July 2009.
- [32] Christian Maaß: *E-Business-Management. Gestaltung von Geschäftsmodellen in der vernetzten Wirtschaft*. 2008, ISBN 978-3-8252-2991-7.
- [33] Sebastian Meissner: *Zertifizierungskriterien für das Datenschutzgütesiegel EuroPriSe*. DuD Datenschutz und Datensicherheit, Seiten 525–531, August 2008.
- [34] The Open Web Application Security Project: *OWASP Top 10 - 2010 release. The Ten Most Critical Web Application Security Risks*. 2010. http://www.owasp.org/index.php/Top_10 , aufgerufen am 12.10.2010.
- [35] Dr. Michael Schmidl: *Aspekte des Rechts der IT-Sicherheit*. Neue Juristische Wochenschrift, Seiten 476–481, 2010.
- [36] Bruce Schneier: *Attack Trees: Modeling Security Threats*. Dr. Dobbs' Journal, December 1999.

-
- [37] Wolfgang Sidler: *Vertrauen schaffen mit zertifizierter Sicherheit: Informations-Sicherheit für KMU*. IT Business, 01/2009, 2009.
- [38] Christof Stych und Klaus Zeppenfeld: *ITIL*. Springer, 2008, ISBN 978-3-540-73118-4.
- [39] TechConsult: *Microsoft Trendbarometer für kleine Unternehmen*. April 2007.
- [40] Frank Victor und Holger Günter: *Optimiertes IT-Management mit ITIL*. vieweg Verlag, 2. Auflage, 2005, ISBN 3-528-15894-8.